Cybersecurity Fundamentals

Information security (InfoSec) is the protection of important information against unauthorized access, disclosure, use, alteration, or disruption.

Computer security is the practice of protecting an organization's computer assets, whether they are computer systems, networks, digital devices or data from unauthorized access, data leakage, cyberattacks and other malicious activities.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. It encompasses all processes, technologies, and security measures applied to protect information and systems in digital or connected environments, such as networks and the internet, against logical threats.

Vulnerabilities and types

A vulnerability is a flaw, weakness, or security defect in physical, logical, or human assets that can be exploited to compromise the confidentiality, integrity, or availability of systems, data, or services. Some examples of the most common vulnerabilities are:

- **Natural:** These are vulnerabilities caused by natural phenomena or environmental conditions that can compromise the company's infrastructure.
- **Physical:** This refers to weaknesses in the protection of spaces where data is stored or processed, such as lack of access controls, equipment exposed to the public, or poorly protected facilities.
- **In Software:** These are programming errors, incorrect configurations, or lack of updates in operating systems, applications, and services, which can be exploited to compromise security.
- **In Hardware:** These are defects in the physical components of a system, such as design, manufacturing, or maintenance failures.
- **In connection:** Affect the security of data during its transmission through networks or media communication.
- **Human:** These are errors or behaviors that attackers can exploit, such as weak passwords, lack of training, or susceptibility to social engineering techniques.

Malware and types

Malware is a set of malicious programs or codes designed to cause damage, obtain illicit profits for its creator, or compromise devices, systems, or networks. It can manifest in various forms, depending on its purpose and behavior, some examples are:

- **Virus:** All viruses are a type of malware, but not all malwares are a virus. Viruses are programs designed to infect legitimate files, replicate, and spread to other devices.

- **Worm:** It is a malware that can replicate and spread autonomously, often exploiting vulnerabilities in networks.
- **Trojan:** It is a type of malware that is presented as a legitimate or harmless program to deceive the user and achieve its execution. Once activated, it allows the attacker to perform malicious actions.
- **Spyware:** It is designed to collect user information without their consent. This information may include browsing habits, credentials, or sensitive data, and is sometimes used for espionage or sold to third parties.
- **Adware:** Generates and displays unwanted advertisements on the infected device, often with the aim of generating income for the attacker or redirecting the user to dangerous sites.
- **Ransomware:** Encrypts the data of infected devices and demands a ransom, usually in cryptocurrencies, in exchange for the decryption key.
- **Rogue:** It is presented as legitimate security software, deceiving the user with alerts of non-existent infections so that they buy false licenses or download other malwares. Malware has different ways of functioning, but most consist of two essential elements for its execution:
    - **Exploit:** It is a set of instructions, code, or tools designed to take advantage of a specific vulnerability and compromise a system or asset, executing unauthorized actions.
    - **Payload:** It is the malicious load that is executed once the exploit has been successful. It can include actions such as malware installation, data theft, or the creation of backdoors.

Privacy/Anonymity

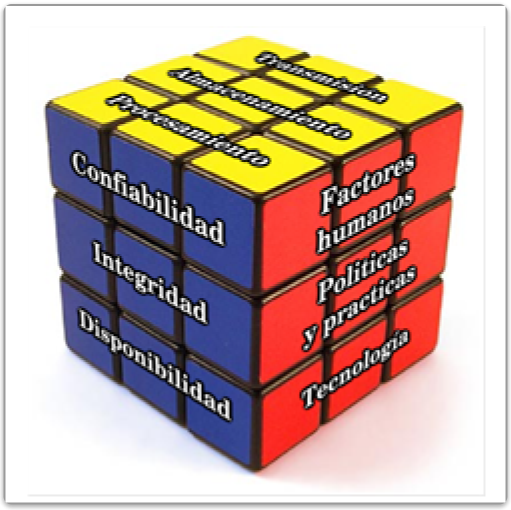
- **Privacy:** Refers to the control that a person or entity has over their personal information. This implies the ability to decide what data to share, with whom to share it, and under what conditions. *Example:* A social network user configures their profile so that only their friends can see their publications.
- **Anonymity:** It is the ability to act or communicate without revealing the identity of the person. Its objective is to protect the individual from personal identity, whether through their name, IP address, digital footprint, or any other identifiable information. *Example:* An activist uses the Tor network to publish a blog about corruption without revealing their identity, protecting themselves from reprisals.

Zero Trust Architecture

It is based on the fundamental principle of **"never trust, always verify"**. Unlike traditional security models that focused on protecting the network perimeter, Zero Trust assumes that threats can originate both from outside and from inside the network. Some key points of this architecture are:

- **Constant verification:** Requires that all users, whether inside or outside the organization's network, are authenticated, authorized, and validated continuously before granting or maintaining access to applications and data.
- **Minimum privilege:** Ensures that employees, equipment, and third parties have access only to the IT resources they strictly need.

McCumber Cube



Security principles

- **Confidentiality:** Refers to protection against unauthorized access to information. It ensures that data is accessible by authorized people, processes, or systems, minimizing the risk of sensitive information leakage *Example:* Encrypt customer information during transmission (SSL/TLS on websites).
- **Integrity:** Ensures that information remains accurate, complete, and reliable over time, preventing unauthorized alterations or damage during storage, transmission, or data processing. *Example:* Use digital signatures to ensure that sent documents have not been altered.
- **Availability:** Seeks to ensure that authorized users can access data and systems when necessary, minimizing downtime or interruptions due to technical failures, attacks, or disasters. *Example:* Backup and failover systems allow services to remain accessible, even during failures.

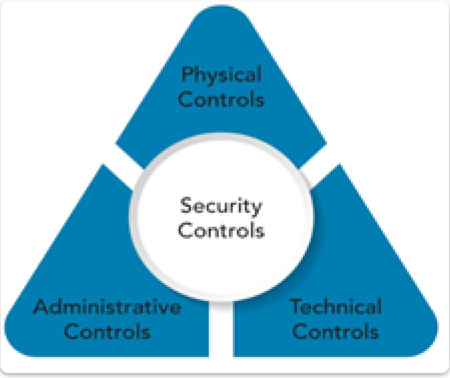
Data status

- **Data in transit:** This is data that is being sent from one place to another, whether within the same network, between networks, or over the Internet. During this state, data is vulnerable to interception and manipulation.
- **Data at rest:** This is data that is stored on local devices or in remote storage. During this state, data is not being processed or transmitted, but must be protected against unauthorized access through encryption and access controls.
- **Data in process:** This is data that is being actively manipulated, such as during input, modification, calculation, or analysis. This state represents the moment when data is most susceptible to errors, malicious alterations, or losses.

Security measures

They are designed to protect an organization's data and infrastructure. For this, they must be based on several fundamental pillars that address different aspects of protection: **Human Factor,** Technology, Policies and Procedures. These pillars ensure that all security elements are integrated and managed effectively.

Security controls



Physical controls

They are designed to protect the physical assets of the organization and prevent unauthorized access to sensitive areas. These include the use of hardware devices such as card readers, biometric access controls, surveillance cameras, perimeter fences, and specific architectural features of buildings, such as armored doors or restricted access systems. In addition, security actions must be carried out by authorized personnel, who must be trained to handle security measures appropriately.

Technical controls

They are security measures implemented directly in the computer systems and networks of the organization. These include automatic protection mechanisms such as firewalls, intrusion detection systems (IDS), data encryption, role-based access control (RBAC), multi-factor authentication (MFA), and patch management policies. In addition, they facilitate the detection of security incidents, allow auditing of accesses and activities, and ensure the protection of sensitive applications and data, both at rest and in transit.

Administrative controls

They are policies, procedures, and directives that regulate the behavior of people within the organization, as well as interactions with external parties. These controls include the implementation of security policies, continuous training in cybersecurity for employees, regulations for the proper handling of sensitive data, incident response policies, and regular audits to ensure compliance.

Defense in depth

Security Onion

It is a model that is based on the idea of multiple layers of security. Each of the layers represents a protection measure (Firewall, IDS, MFA, network segmentation) that an attacker must overcome to compromise the system. The advantage of this model is the redundancy in defenses, which increases the probability of detecting a possible attack. *Example:* An attacker tries to access a corporate server.

But first, they must face a firewall, then an intrusion detector (IDS), and finally, multi-factor authentication (MFA). These layers must be overcome to compromise the system.

Security Artichoke

In this model, each of the defense layers can contain sensitive information, which implies that it is not necessary to reach the core of the system to extract valuable data. This highlights the importance of adequately securing each layer, avoiding information leaks in superficial points. *Example:* An employee neglects to protect some data in a shared system. Although the attacker only compromises one layer, they can access relevant company data without needing to evade other security systems.

Risk management

It is an essential strategic process for organizations seeking to protect their digital assets and ensure the continuity of their operations. It consists of identifying, analyzing, evaluating, and mitigating the threats that lurk in information systems. The main objective is to establish preventive controls and reduce exposure to possible security incidents.

Key stages in cybersecurity risk management

1. **Risk identification:** The first step is to recognize and document the possible threats and vulnerabilities that could affect the organization. This implies a deep knowledge of the information assets and possible weak points in the cybersecurity infrastructure.
2. **Analysis and Evaluation:** Once the risks have been identified, they are analyzed to understand their possible impact on the organization. The probability of them occurring and the potential damage they could cause to digital assets and business operations is evaluated.
3. **Management and Mitigation:** In this stage, strategies are defined and applied to treat the identified risks. This may include the implementation of security controls, the transfer of risk (such as cyber insurance) or the acceptance of risk when the cost of mitigation is too high compared to the potential impact.
4. **Monitoring and Review:** Risk management is an ongoing process. It is essential to constantly monitor the threat landscape, review the effectiveness of the implemented controls, and adjust risk management strategies as necessary to adapt to new challenges and vulnerabilities.

Incident response

It is the set of processes and actions that an organization must carry out to detect, contain, eradicate, and recover from a computer security incident. It is a critical function to minimize damage and restore normal operations as quickly as possible after a cyberattack.

Key phases in incident response

1. **Preparation:** Before an incident occurs, it is essential to establish an incident response plan. This includes defining roles and responsibilities, establishing communication procedures, identifying critical assets, and configuring the necessary tools and technologies for detection and response.

2. **Detection and Analysis:** This phase focuses on identifying the occurrence of a security incident. It involves continuous monitoring of systems and networks, analysis of security alerts, and evaluation of possible suspicious events to confirm whether it is a real incident and determine its scope and nature.
3. **Containment:** Once an incident has been confirmed, the main objective is to prevent it from spreading and minimize its impact. Containment actions may include isolating affected systems, segmenting networks, disabling compromised services, or modifying firewall rules.
4. **Eradication:** This phase focuses on eliminating the root cause of the incident and restoring systems to a secure state. It may involve removing malware, correcting vulnerabilities, rebuilding compromised systems, or restoring data from backups.
5. **Recovery:** The objective of this phase is to restore the organization's normal operations as quickly as possible. It includes the recovery of systems and data, the validation of the security of the restored systems, and the gradual resumption of the affected services.
6. **Lessons Learned (Post-incident):** After resolving the incident, it is crucial to conduct a post-incident review to analyze what happened, identify the root causes, evaluate the effectiveness of the response, and document the lessons learned. These lessons should be used to improve the incident response plan and strengthen the organization's security posture.

Access control models

Discretionary Access Control (DAC)

It is the least restrictive model and allows users to control access to their data as if they were owners of that data, they can use an ACL or other methods to specify which users or groups of users have access to the information.

Mandatory Access Control (MAC)

The strictest access control is applied and is often used in military or mission-critical applications, assigns security level labels to information, and enables user access based on the level of authorization.

Role-Based Access Control (RBAC)

Access decisions are based on the roles and responsibilities of the individual within the organization, security privileges are assigned to different roles, and people are assigned to the RBAC profile for the role. Roles can include different positions, job classifications, or groups of job classifications.

Attribute-Based Access Control (ABAC)

It allows access based on the attributes of the object (resource) that will be accessed, the subject (user) that will access the resource, and the environmental factors regarding how the object will be accessed.

Rule-Based Access Control (RuBAC)

Network security personnel specifies sets of rules or conditions associated with access to data or systems. These rules can specify allowed or denied IP addresses, or certain protocols and other conditions.

Time-Based Access Control (TAC)

Allows access to network resources based on the time and day.

Authentication protocols

Extensible Authentication Protocol (EAP)

The client's password is sent using a hash to the authentication server. The authentication server has a certificate.

Password Authentication Protocol (PAP)

A username and password are sent to a remote access server in plain text. Most network operating system servers support PAP. It is an insecure protocol as it transmits the information in plain text.

Challenge Handshake Authentication Protocol (CHAP)

CHAP validates the identity of remote clients using a one-way hash function created by the client. The service also calculates the expected hash value. The server compares the 2 values, if both match, the transmission continues. It also periodically verifies the client's identity during the transmission.

Authentication technologies

802.1x

An organization authenticates its identity and authorizes access to the network. Their identity is determined based on credentials or a certificate confirmed by a RADIUS server.

RADIUS

When username/password authentication is needed, RADIUS is used to accept or deny access. This service only encrypts the user's password from the RADIUS client to the RADIUS server. The username, usage log, and authorized services are transmitted in plain text. When this technology is implemented, only security measures that protect against replay attacks are necessary.

TACACS+

Uses TCP as a transport protocol. It encrypts all data between the client and server. Since network administrators can define ACLs, filters, and user privileges, it is the best option for corporate networks that require more sophisticated authentication steps and control over authorization activities.

Kerberos

Kerberos uses strong encryption, requiring a client to prove its identity to a server, and the server in turn authenticates itself to the client. The Kerberos server contains user IDs and hashed passwords for all users who will have authorizations for the domain services. The Kerberos server also has shared secret keys with all the servers to which it will grant access tickets. The first ticket is a ticket-granting ticket issued by the authentication service to a requesting client. The client can present this ticket to the Kerberos server with a request for a ticket to access a specific server. By being able to encrypt the entire session, the intrinsically insecure transmission of elements that can be intercepted on the network is eliminated. Tickets have an expiration date, so any attempt to reuse a ticket will not be successful.

AAA Operation

The Authentication, Authorization, and Accounting (AAA) protocol provides the framework needed to enable scalable access security.

Authentication

Users and administrators must prove that they are who they claim to be, authentication can be established using combinations of username and passwords, challenge questions and answers, token cards, and other methods. Authentication provides a centralized way to control network access.

Authorization

Once the user is authenticated, the authorization services determine which resources the user can access and what operation they are enabled to perform.

Accounting

Accounting records also have the function of recording what the user does, including the elements they access, the amount of time they access the resource, and all the changes that were made. Accounting tracks how network resources are used.