Ch.9 summary By @MHazazi

Access Control Fundamentals

- **Access controls**
  - Security features that govern how users and processes communicate and interact with systems and resources
  - Primary objective is to protect information and systems from unauthorized access, modification, or disruption
  - **subject** = Active entity (user or system) that requests access to a resource or data
  - **object** = Passive entity being accessed or being acted upon
- **Three common attributes of access controls**
  1) **Identification scheme** = used to identify unique records in a set, such as a user name.
     Identification is the process of the subject supplying an identifier to the object.
  2) **Authentication method =** how identification is proven to be genuine.
     Authentication is the process of the subject supplying verifiable credentials to the object.
  3) **Authorization method =** how access rights and permission are granted.
     Authorization is the process of assigning authenticated subjects the permission to carry out a specific operation
- **The security posture of an organization determines the default settings for access controls.**
- **Access controls can be:**
  - Technical (such as firewalls or passwords),
  - Administrative (such as separation of duties or dual controls),
  - Physical (such as locks, bollards, or turnstiles).

What Is a Security Posture?

- **Security posture** is an organization's approach to access controls
- **Fundamental postures are:**
  - **Open** (default allow) = access not explicitly forbidden, is permitted.
  - **Secure** (default deny)= access not explicitly permitted, is forbidden.
- Every access control decision for a company is based on that company's security posture

Open (default allow)	**Secure** (default deny)
- Easy to deploy ,Work out-of-the-box - Everyone can do everything - No security is deployed	- deny all - Access is unavailable by default until the appropriate control is altered to allow access

➢ **Principle of Least Privilege**

- The least amount of permissions granted to users while still allow them to perform the required business tasks and no more.
- This is a strong foundation for any access control policy.
- Protects the data but also protects users.
- it is important to explain to employees why they are not "trusted" to gain all permission

➢ **Principle of Need-to-know**

- Having a demonstrated and authorized reason for being granted access to information
- Should be made a part of the company's culture
- Should be incorporated in security training curriculum
- At the least protects the confidentiality of corporate data, but may also protect integrity and availability depending on the attack type

How Is Identity Verified?

➢ First step to granting access is user identification

➢ **Authentication**: Subject must supply verifiable credentials(factors)

Factor	Brief	Example
Knowledge	Something you know Most common factor to use and the easiest to beat. Considered single-factor authentication.	Password PIN Answer question
Possession	Something you have Prove your identity by something you own it and use it during authentication. Considered multi-factor authentication	Smart card Token
Inherence	Something you are Use Biometric methods, which you are the only person who has it. This factor offers strongest authentication but its susceptible to errors depend on its sensitivity.	Fingerprints iris scans

■ Single-factor authentication = only one factor is presented

■ Multifactor authentication = two or more factors are presented

■ Multilayer authentication = two or more of the same type of factors are presented

What Is Authorization

- The process of assigning authenticated subjects permission to carry out a specific operation
- **Three primary authorization models:**
  1) **Object capability**
     programmatically and based on a combination of unforgettable reference and an operational message
  2) **Security labels**
     Mandatory access controls embedded in object and subject properties
  3) **Access Control Lists**
     Used to determine access based on some criteria
- **Categories of access control lists**
  - **MAC (Mandatory Access Control):**
    Data is classified, and employees granted access according to the sensitivity of information
  - **DAC (Discretionary Access Control):**
    Data owners decide who should have access to what information
  - **RBAC (Role-based Access Control):**
    Access is based on positions (roles) within an organization
  - **Rule-based access control:**
    Access is based on criteria that is independent of the user or group account

Infrastructure Access Controls

- Include physical and logical network design, border devices, communication mechanisms, and host security settings
- **Network segmentation**
  - The process of logically grouping network assets, resources, and applications
  - **Type of network segmentation:**
    - Enclave network = segment of internal network requires high protection
    - Trusted network = internal network accessible to authorized users
    - Semi-trusted, perimeter, or DMZ network = designed to be accessed through internet
    - Guest network = designed for use by visitors to connect to the Internet
    - Untrusted network = network outside your security controls

What Is Layered Border Security?

- Different types of security measures designed to work in tandem with a single focus
  - **Firewall devices =** device or software that control the flow of traffic between networks.
  - **Intrusion detection systems (IDSs) =** passive devices analyze network traffic to detect unauthorized access
  - **Intrusion prevention systems (IPSs) =** active devices sit inline with traffic flow and respond to identified threats by disabling the connection, dropping the packet, or deleting the malicious content
  - **Content filtering and whitelisting/blacklisting =** applications used to restrict access by content category
  - **Border device administration and management =** used for monitoring and administration

Remote Access Security

- **Remote Access**
  - Users with business-need to access the corporate network remotely and are authorized to do so must be given that privilege
  - Not all employees should be given this privilege by default
  - Remote access activities should be monitored and audited
  - The organization's business continuity plan must account for the telecommuting environment
- **Remote access technologies**
  - Virtual Private Networks (VPNs)
    - Secure tunnel for transmitting data over unsecure network, such as the Internet
  - Remote access portals
    - Offers access to one or more applications through a single centralized interface

User Access Controls

- Used to ensure authorized users can access information and resources while unauthorized cannot
- Users should have access only to information they need to do their job and no more
- Administrative account controls
  - Segregation of duties
  - Dual control
- **Three main monitoring areas:**
  - Successful access
  - Failed access
  - Privileged operations

Is Monitoring Legal

- Courts indicate that monitoring is acceptable if it is reasonable:
  - Justifiable if serving a business purpose
  - Policies are set forth to define what privacy employees should expect while on company
  - Employees are made aware of what monitoring means are deployed
- Acceptable use agreement should include a clause informing users that the company will and does monitor system activity.
- Users must agree to company policies when logging on