Chapter 2: Pervasive Attack Surface and Controls

Social Engineering Attacks

- **Social engineering** is a means of eliciting information or convincing a user to take action that weakens security
  - It is almost always performed through deception and manipulation of the user
- It is said to be accomplished using human vectors as the attack surface

Examples of Human Manipulation

- Social engineering relies heavily on human psychology
- Attackers use a variety of techniques to gain trust:
  - **Provide a reason**
  - **Project confidence**
  - **Use evasion and diversion**
  - **Make them laugh**

Types of Social Engineering Attacks

- **Phishing** is sending an email message or displaying a web announcement that falsely claims to be from a legitimate source in an attempt to trick the user into taking an action
- Variations on phishing attacks include the following:
  - **Spear phishing**
  - **Whaling**
  - **Vishing**
  - **Smishing**

Types of Social Engineering Attacks

- Social engineering **impersonation** is masquerading as a real or fictitious character and then playing out the role of that person on a target
- One type of impersonation is **brand impersonation** where a threat actor pretends in order to build immediate recognition and trust
- Redirection is when an attacker directs a user to a fake lookalike site filled with ads for which the attacker receives money for traffic generated to the site
  - Two types of redirection are known as type squatting and pharming

Types of Social Engineering Attacks

- **Misinformation** is false or inaccurate information and **disinformation** is false or inaccurate information that comes from a malicious intent
- An example of cyber disinformation is a **hoax** or a false warning
- A **watering hole attack** is directed toward a smaller group of specific individuals, such as the major executives working for a manufacturing company
  - These executives all tend to visit a common website that an attacker may try to infect with malware

Types of Social Engineering Attacks

- The following are other means by which a threat actor can gather valuable information:
  - **Dumpster diving** involves digging through trash receptacles to find information that can be useful in an attack
  - **Google dorking** uses advanced Google search techniques to look for information that unsuspecting victims have carelessly posted on the web
  - **Shoulder surfing** occurs when a user casually observes someone entering secret information without drawing attention to themselves

Perimeter Defenses

- Some organizations have used “industrial camouflage” to make the physical presence of a building as nondescript as possible
- Perimeter defenses must be used to restrict access
- This type of defense includes barriers, security guards, sensors, security buffers, and locks

Barriers

- **Fencing** is usually a tall, permanent structure to keep out unauthorized personnel
  - Most modern perimeter security consists of a fence equipped with other deterrents
- A **bollard** is a short but sturdy vertical post that is used as a vehicular traffic barricade to prevent a car from “ramming” into a secure area

Security Guards

- Human **security guards** who patrol and monitor restricted areas are an active security defense
  - Two security guards may be required for a higher level of protection (called **two-person integrity/control**)
- Often guards monitor activity captured by **video surveillance** cameras
  - High-end video surveillance cameras send alerts and begin recording when they detect movement or identify a suspicious object
- Drones, called unmanned aerial vehicles (UAVs) are being used for monitoring activity

Sensors

- An infrared (IR) sensor is an electronic device that can measure and detect IR in the surrounding area
- A technology that can be used to monitor a large area is a microwave sensor, which uses high-frequency radio waves and functions similarly to radar
- Ultrasonic sensors can measure how far away a target object is located
  - They are not as susceptible to interference by smoke, gas, and other airborne particles

Security Buffers

- A **buffer** serves as a protective barrier to provide an additional layer of security to keep intruders from entering areas but still show approved personnel
  - A **mantrap** is a security buffer where a user shows credentials to open the first door where their credentials can be checked before a second door that they must pass through is unlocked
- In areas in which medium security is needed, a **reception area** can be used
- In areas of low security, a generic **waiting room** can be used instead

Preventing Data Leakage

- Another means of physical security applies to preventing important data from escaping (leakage)
- The following physical controls can be applied:
  - Faraday cage and protected cable distribution systems

Faraday Cage

- Electronic devices emit electromagnetic fields which can result in interference called **electromagnetic interference** (**EMI**)
  - Unauthorized persons could detect and read these electromagnetic signals
- A Faraday cage is a metallic enclosure that prevents the entry or escape of an electromagnetic field
- Lightweight and portable **Faraday bags** made of special materials can be used to shield portable devices

Protected Distribution System

- A **protected distribution system** (**PDS**) is a system of cable conduits used to protect classified information transmitted between two secure areas
- Two types of PDSs are commonly used:
  - In a **hardened carrier PDS**, the data cables are installed in a conduit that is constructed of special electrical metallic tubing
  - In an **alarmed carrier PDS**, the carrier system is deployed with specialized optical fibers in the conduit that can sense acoustic vibrations that occur when an intruder attempts to gain access to the cables, which triggers an alarm

Data Controls

- It is imperative to have adequate controls in place to protect data
- Protecting data involves knowing the different classifications and types of data, the consequences of a data breach, and controls for protecting data

Data Classifications

Data type	Description	Recommended handling
Confidential	Highest level of data sensitivity	Should only be made available to users with the highest level of preapproved authentication
Private	Restricted data with a medium level of confidentiality	For users who have a need-to-know basis of the contents
Sensitive	Data that could cause catastrophic harm to the company if disclosed, such as technical specifications for a new product	Restricted to employees who have a business need to access the data and have been approved
Critical	Data classified according to availability needs; if critical data are not available, the function and mission would be severely impacted	Critical data must be rigorously protected
Public	No risk of release	For all public consumption; data is assumed to be public if no other data label is attached
Restricted	Data that is not available to the public	Caution should be exercised before using this kind of information in emails

Types of Data

- **Regulated data** is that which external stipulations are placed on it regarding who can see and use the data and in what contexts
- **Intellectual property** (**IP**) **data** is an invention or a work that is the result of creativity
- **Trade secret data** is enterprise data that is undisclosed
- **Legal information** is general factual information about the law and the legal process
- **Financial information** is data about the monetary transactions of the enterprise

Types of Data

- **Human-readable data** is that which a person can read and interpret
- **Non-human-readable data** (also called **machine-readable**) is data that a device can “interpret” and in its native state is not readily understood by a person
- An example of non-human-readable data is JavaScript object notation (JSON)

Data Breach Consequences

- The following are possible consequences to an organization that has suffered a data breach:
  - Reputation damage
  - IP theft
  - Fines

Protecting Data

- Several general considerations about data should be taken into account prior to creating data controls
- The first consideration is the **data state** or its condition
- The following are three states in which it may reside:
  - Data in processing
  - Data in transit
  - Data at rest

Protecting Data

- Another consideration is where the data is located
  - **Geolocation** is a term encompassing all techniques that identify the data's location
- **Data sovereignty** is the country-specific requirements that apply to data
  - Data is subject to the laws of the country in which it is collected or processed

Data Security Methods

- Techniques to enhance the protection of data include the following:
  - Data minimization
  - Data masking
  - Tokenization
  - Restrictions
  - Segmentation