Threats and Attacks

Madiba Hudson-Quansah

Contents

Chapter 1

Threat Categories

Definition 1.0.1: Threat

A threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.

There are 12 categories of threats:

- Compromises to Intellectual Property
- Deviations in quality of service
- Espionage / Trespass
- Forces of Nature
- Human error / Failure
- Information Extortion
- Sabotage / Vandalism
- Technical Hardware failures / Errors
- Technical Software failures / Errors
- Technological Obsolescence

1.1 Compromises to Intellectual Property

Definition 1.1.1: Intellectual Property

Creation, ownership, and control of original ideas, information, and creative works.

IP breaches compromise the **Confidentiality** of information, some examples are piracy, and copyright infringement.

1.1.1 Technical Controls

- Watermarking
- Embedded Code
- Registration Keys
- Intentional Corruption
- Obfuscation

1.1.2 Administrative/Legal Controls

- End User License Agreements (EULA)
- Copyrights
- Licenses

1.2 Deviations in Quality of Service

Deviations in quality of service occur when products or services are not delivered as expected, this compromises the **Availability** of a system. This is commonly cause by:

- Failure of interdependent support systems
- Supply Chain failures
- Failure of critical infrastructure (e.g power grid)

1.2.1 Technical Controls

- Redundancy
- Failover Systems / Redundant Systems (e.g. Redundant Array of Independent Disks (RAID))
- Backup Internet Service Providers (ISPs)
- Load Balancing
- Cloud Geographic Distribution

1.2.2 Administrative Controls

- Service Level Agreements (SLAs) - Contract between service provider and customer that specifies the level of service expected during its term.
- Policies and Procedures to deal with QoS issues

1.3 Espionage / Trespass

Definition 1.3.1: Espionage / Spying

Gaining unauthorized access to the information of an organization. The practice of obtaining information about an organization without the permission of the holder of the information.

Definition 1.3.2: Trespass

The act of entering someone's land or property without permission.

Espionage and Trespass primarily compromise the **Confidentiality**. Some examples include:

- Shoulder Surfing - Observing a person's private information over their shoulder.
- Industrial Espionage
- Hacking
- Governmental Espionage
- Social Engineering

1.4 Information Extortion / Cyberextortion

An attacker steals information from a computer system and demands compensation for it's return or non-disclosure. Cyberextortion primarily compromises **Availability**, then **Integrity** and **Confidentiality** if data is exfiltrated. There are two types of ransomware attacks:

- Lock screen - Prevents access to the device
- Encryption - Encryptions sensitive files

1.4.1 Technical Controls

- Anti-Malware Software
- Email and Web Filtering
- Data Backups

1.4.2 Administrative Controls

- User Training
- Incident Response Plan
- Regular Software Updates and Patch Management

1.5 Sabotage / Vandalism

Definition 1.5.1: Sabotage

The obstruction of a system's operations or intended functions. Sabotage is often directed with an explicit reason / goal.

Definition 1.5.2: Vandalism

The intentional destruction or defacement of property. The main intention of vandalism is destruction.

Involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy and asset or damage the image of an organization. This primarily compromises **Integrity** and **Availability**. Some examples include:

- Website defacing - Erodes consumer confidence
- Hacktivism / Cyberactivism
- Cyberterrorism / Cyberwarfare.

1.5.1 Technological Controls

- Web Application Firewalls (WAF)
- Distributed Denial of Service (DDoS) protection
- Website defacement monitoring
- Backups

1.5.2 Administrative Controls

- Policies and Procedures
- Legal Enforcement
- Awareness Training

1.5.3 Operational Controls

- Physical security of equipment.
- Host Redundancy
- Incident Response
- Monitoring

1.6 Software Attacks

Definition 1.6.1: Malware

Malicious software designed to infiltrate or damage a computer system without the owner's informed consent.

Involve designing and deploying malware to compromise a system. Software attacks may overwhelm the processing capabilities of online systems or allow access to protected systems by hidden means. Software attacks primarily compromise **Confidentiality**, **Integrity**, and **Availability** to varying severities. Some examples include:

Traditinoal Malware Viruses, Worms, Trojans, Spyware, Adware, Ransomware, Rootkits, Keyloggers

Access/Control Malware Backdoors, Botnets, Remote Access Trojans (RATs)

Disruption Attacks Denial of Service (DoS), Distributed Denial of Service (DDoS)

Interception Attacks Spoofing, Man-In-the-Middle (MitM), Session Hijacking, Packet sniffing, pharming

Definition 1.6.2: Viruses

A type of malware that attaches itself to a legitimate program or file and spreads to other programs and files when executed.

Definition 1.6.3: Worm

A type of malware that can replicate itself and spread independently without needing to attach to a host program.

Definition 1.6.4: Trojan

A type of malware that disguises itself as a legitimate program or file to trick users into installing it, often creating a backdoor for unauthorized access.

Definition 1.6.5: Logic Bomb

A type of malware that is triggered by a specific event or condition, such as a date or the deletion of a file.

Definition 1.6.6: Zero-Day Attack

An attack that exploits a previously unknown vulnerability in a computer application, meaning there is no existing patch or fix for the vulnerability.

Definition 1.6.7: Pharming

A cyberattack that redirects a website's traffic to a fraudulent website, often through DNS cache poisoning or modifying the hosts file on a victim's computer.

Definition 1.6.8: Phising

A cyberattack that uses fraudulent emails or websites to trick individuals into revealing sensitive information, such as passwords or credit card numbers.

1.6.1 Technical Controls

- Anti-Virus / Anti-Malware Software
- Firewalls
- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
- Patch Management
- Secure Software Development Practices

1.6.2 Administrative Controls

- Security Policies on patching
- User Training
- Software Inventory Management

1.6.3 Operational Controls

- Incident Response Planning and Policies
- Malware Analysis Teams
- Threat Intelligence Sharing
- Backups

1.7 Technical Hardware Failures / Errors

Occurs when a manufacturer distributes equipment containing a known or unknown flaw. This primarily compromises **Availability** and **Integrity**. Some examples include:

- Pentium II Floating Point Division Bug
- Spectre and Meltdown CPU Vulnerabilities
- Hardware crashes
- RAM failures

1.7.1 Technical Controls

- Redundancy (e.g RAID)
- Error Checking RAM
- Uninterruptible Power Supplies (UPS)

1.7.2 Administrative Controls

- Vendor Risk Assessment
- Procurement Policies
- Warranty and Maintenance Agreements

1.7.3 Operational Controls

- Preventative Maintenance Schedules
- Hardware Monitoring Tools
- Asset Lifecycle Management