Sprint 2 Part 2 Identifying Potential Threats

Cybersecurity threats within an organization

In general, organizations need to protect sensitive data such as customer information, financial data, and intellectual property. The organization's business model may also impact their cybersecurity needs, as some models may require more advanced security measures than others. For example, an e-commerce business that stores credit card information will have more security needs than a small firm.

Cyber-attacks are constantly evolving, so it's important to stay up-to-date on the latest threats and vulnerabilities. Here are a few of the latest threats:

1. **Ransomware:** This type of malware encrypts a victim's files and demands a ransom in exchange for the decryption key. Ransomware attacks have become increasingly common and can be devastating for organizations that don't have proper backups or security measures in place.

2. **Phishing:** Phishing attacks involve sending fake emails or messages that appear to be from a legitimate source, such as a bank or company, in an attempt to trick the recipient into revealing sensitive information or downloading malware. Phishing attacks can be difficult to spot and can cause significant damage.

3. **Zero-day exploits:** Zero-day exploits are vulnerabilities in software that are unknown to the software vendor and can be exploited by attackers. These exploits can be used to gain access to systems or steal sensitive data.

4. **Advanced persistent threats (APTs):** APTs are targeted attacks that are designed to gain long-term access to a network or system. APTs can be difficult to detect and can remain active for months or even years, allowing attackers to steal sensitive data over an extended period of time.

To protect against these and other cybersecurity threats, organizations should have a proper cybersecurity strategy in place that includes measures such as regular software updates, employee training on cybersecurity best practices, and the use of advanced security tools like firewalls, intrusion detection systems, and antivirus software. It's important to have a plan in place as well for responding to cybersecurity incidents, including data breaches and other attacks.

Threat Actors

A threat actor is an individual or group posing a threat. Everyday the threat landscape is growing and not only are organizations like businesses being attacked but your average citizen/homeowner should be worried also. Threat actors will use a combination of different techniques and tactics to carry out attacks, and will always evolve over time to bypass security measures

There are several types of threat actors that may target an organization, including:

Hackers: These are individuals or groups who gain unauthorized access to an organization's systems, networks, and data with the intent of stealing or manipulating information.

Cybercriminals: These are individuals or groups who engage in illegal activities online for financial gain, such as stealing credit card information or conducting ransomware attacks.

Nation-state actors: These are individuals or groups who are sponsored by a nation-state government and carry out cyber attacks to gather intelligence or disrupt operations of other countries.

Insiders: These are employees or contractors who have authorized access to an organization's systems and data but use that access for malicious purposes, such as stealing sensitive information or disrupting operations.

Hacktivists: These are individuals or groups who use hacking techniques to promote a political or social agenda and may target organizations that they view as opposing their beliefs or causes.

Terrorists: These are individuals or groups who may use cyber attacks as part of a larger campaign of violence or to create fear and disruption.

Script kiddies: These are individuals who use pre-packaged automated tools and scripts to launch simple attacks against organizations for fun or to prove their skills.

Data Threats Internal vs External

Internal threats to an organization's data come from employees, contractors, or anyone who has access to the organization's systems and data. These threats include:

1. **Malicious employees:** Employees who intentionally try to steal or damage the organization's data.

2. **Unintentional actions:** Accidents or mistakes that cause data loss or damage, such as accidentally deleting files or the misconfiguration of systems.

3. **Insider threats:** Employees who inadvertently or intentionally share sensitive data with unauthorized third parties.

4. **Unauthorized access:** Employees who access data they are not authorized to view, such as confidential HR files or customer data.

5. **Weak passwords and poor security practices:** Employees who use weak passwords, reuse passwords, or engage in poor security practices that can make it easier for hackers to gain access to data.

External threats to an organization's data come from outside the organization and can include:

1. **Cybercriminals**: Individuals or groups who attempt to breach the organization's security systems to steal data, disrupt operations, or hold data for ransom.

2. **Hacktivists:** Individuals or groups who attempt to disrupt or damage an organization's operations for political or ideological reasons.

3. **Nation-state actors:** Governments or government-sponsored groups who attempt to steal sensitive data for intelligence or military purposes.

4. **Natural disasters:** Events such as floods, earthquakes, or fires that can damage physical infrastructure and lead to data loss.

5. **Third-party vendors:** External vendors or service providers who may have access to the organization's data, but who may not have the same level of security controls in place as the organization itself.

Data Threat Vectors

There are many threat vectors that threat actors can use to compromise an organization's data, some of these would be:

1. **Phishing attacks:** These attacks typically involve sending fraudulent emails or other types of messages to employees, attempting to trick them into providing login credentials or other sensitive information.

2. **Malware attacks:** Malware is malicious software that can infect a computer or network and steal data, corrupt files, or cause other types of damage. Malware can be delivered via email attachments, malicious links, or infected websites.

3. **Social engineering attacks:** Social engineering is the use of psychological manipulation to convince individuals to disclose sensitive information or perform actions that could compromise the security of an organization's data.

4. **Insider threats:** Employees or other insiders with access to an organization's data can pose a significant threat if they engage in malicious activities or accidentally expose sensitive information.

5. **Physical attacks:** Physical attacks involve gaining access to an organization's premises or IT infrastructure to steal or compromise data. This could include stealing laptops, hacking into servers, or tampering with network equipment.

6. **Advanced persistent threats (APTs):** APTs are targeted attacks that involve highly sophisticated tactics, such as zero-day exploits or custom malware, to gain access to an organization's data and remain undetected for long periods of time.

7. **Denial-of-service attacks (DoS):** DoS attacks are designed to overwhelm an organization's servers or network infrastructure, rendering them unavailable and causing disruption to business operations.

A threat vector is a path or means by which a cybercriminal can use to gain access through one or more routes into a system. To mitigate these threats an organization should use a secure cybersecurity program, regular employee training and password policies as well as incident response planning are all valid ways to help build security within the program.