|  |
| --- |
| Name: Tom Wang Her suen  Assignment 4 |

## Assignment 4

**Discuss and present a Security Vulnerability and Cyberattacks incident**

* What happened?
* What is the effect?
* How it did happen?
* How did they solve the problem?
* How can we prevent this from happening again?

**Topic Example:**

* 2010 - WeWork Network Vulnerabilities

| **Incident** | **What Happened?** | **Effect** | **How It Happened?** | **How They Solved the Problem?** | **Prevention Measures** |
| --- | --- | --- | --- | --- | --- |
| **2021 - XYZ Corp Ransomware Attack** | A ransomware attack targeted XYZ Corp's IT infrastructure. | Critical data encrypted, leading to operational disruption. | Phishing email delivered malware, exploiting vulnerabilities. | XYZ Corp paid the ransom to decrypt data and restore systems. | - Conduct regular employee training on phishing awareness. |
|  |  |  | Lack of patching and updates in the network infrastructure. | Restored from backups, implemented enhanced cybersecurity. | - Keep software and systems updated with the latest patches. |
|  |  |  | Weak access controls and inadequate network monitoring. | Engaged with cybersecurity experts to analyze and secure systems. | - Implement multi-factor authentication for access controls. |
|  |  |  | Inadequate backup and recovery mechanisms. | Strengthened backup and recovery processes and systems. | - Regularly test and validate backup and recovery procedures. |
|  |  |  | Limited incident response and recovery planning. | Developed and implemented an incident response plan. | - Establish and regularly test an incident response framework. |

1. In this example, the incident involves a ransomware attack on Wechat Corp in the year 2021. The table outlines what happened, the effects, the causes of the incident, how the organization addressed the problem, and preventive measures to avoid similar incidents in the future. Each incident is unique, and real incidents may involve different factors and responses.
2. **What Happened?**
   * A ransomware attack targeted XYZ Corp's IT infrastructure.
3. **Effect:**
   * Critical data was encrypted, leading to operational disruption.
4. **How It Happened?**
   * The attack vector was a phishing email that delivered malware.
   * The malware exploited vulnerabilities in the network infrastructure.
   * Weak access controls and inadequate network monitoring allowed the attack to propagate.
   * Lack of patching and updates in the network infrastructure created entry points for the attackers.
5. **How They Solved the Problem?**
   * XYZ Corp paid the ransom to decrypt data and restore systems.
   * Restored systems from backups.
   * Implemented enhanced cybersecurity measures, including regular patching.
   * Engaged with cybersecurity experts to analyze and secure systems.
   * Strengthened backup and recovery processes and systems.
   * Developed and implemented an incident response plan.
6. **Prevention Measures:**
   * Conduct regular employee training on phishing awareness to reduce the likelihood of falling victim to phishing attacks.
   * Keep software and systems updated with the latest patches to address known vulnerabilities.
   * Implement multi-factor authentication for access controls to enhance security.
   * Regularly test and validate backup and recovery procedures to ensure their effectiveness.
   * Establish and regularly test an incident response framework for effective response and recovery.

This detailed breakdown provides insights into the incident, its effects, the root causes, the response strategies, and preventive measures that XYZ Corp could take to avoid a similar incident in the future. It emphasizes the importance of a multi-layered approach to cybersecurity, including employee education, system updates, access controls, backup procedures, and incident response planning.