**Lab Tutorial: Cyberattack Case Study and Mitigation Strategies**

**Lab Duration:** 1 Hour  
**Objective:** Analyze a recent cyberattack, determine its root cause, and propose mitigation strategies.

**Lab Overview:**

In this lab, students will conduct a case study on a recent cyberattack. Each student can choose a cyberattack from the list provided. The goal is to understand how the attack occurred, what vulnerabilities were exploited, and how similar attacks can be prevented.

You are required to formally record your details in this document instead of solely getting information from the web server. This document should be present in your weekly code folder.

**Lab Instructions:**

**Step 1: Choose an Attack**

Each student should select one of the following cyberattacks:

1. **SolarWinds Supply Chain Attack (2020)** – Attackers inserted a backdoor into SolarWinds' Orion software, impacting thousands of organizations.
2. **Colonial Pipeline Ransomware Attack (2021)** – A ransomware attack disrupted fuel supply on the East Coast of the U.S.
3. **Log4j Vulnerability Exploit (2021)** – A critical flaw in Log4j allowed remote code execution across various systems.
4. **Twitter Bitcoin Scam (2020)** – Hackers gained access to high-profile Twitter accounts and promoted a Bitcoin scam.
5. **Uber Data Breach (2022)** – Social engineering led to unauthorized access to Uber’s internal systems.
6. **T-Mobile Data Breach (2023)** – Attackers exploited API vulnerabilities to steal customer data.
7. **CrowdStrike IT Outages (2024) –** In March 2024, following a stress test, CrowdStrike released Rapid Response Content for Channel File 291. Subsequent updates in April 2024 led to IT outages for some customers, prompting investigations and clarifications from the company.
8. **Microsoft Exchange Server Hack (2021)** – State-sponsored hackers exploited vulnerabilities in Microsoft Exchange servers.
9. **MOVEit File Transfer Hack (2023)** – A zero-day vulnerability in MOVEit file transfer software was exploited to steal data.
10. **WannaCry Ransomware Attack (2017)** – A global ransomware attack exploited a vulnerability in Microsoft Windows, impacting thousands of organizations worldwide, including the NHS in the UK.
11. **Zoom Security Issues (2020)** – During the rise of remote work, cybercriminals exploited flaws in Zoom’s video conferencing software, leading to "Zoombombing" incidents and concerns over encryption.
12. **23andMe data breach (2022) -** An unauthorized party gained access to the personal data of some of the genetic testing company's users.
13. **Kaseya VSA Ransomware Attack (2021)** – Attackers targeted the Kaseya VSA platform, which is used by managed service providers, infecting their clients with ransomware. This attack impacted hundreds of businesses and organizations globally.

**Step 2: Research the Attack**

1. **How did the attack happen?** Identify the vulnerabilities or weaknesses exploited.
2. **Who were the attackers?** (If known) Identify whether it was a nation-state, criminal group, or individual hackers.
3. **What was the impact?** Discuss the financial, operational, and reputational damage.
4. **How was it discovered?** Explain how organizations or security researchers identified the attack.

**Step 3: Determine the Cause and Mitigation**

1. **Why did the attack succeed?** Identify security gaps, misconfigurations, or lack of updates.
2. **How could it have been prevented?** Suggest security best practices and solutions.
3. **What mitigation strategies should be in place to prevent future attacks?** Discuss security controls like network monitoring, incident response plans, and user awareness training.

**Step 4:** Work with at least one of your peer and share your findings to them

**Lab Logbook Requirement:** Record the following in your lab logbook:

1. The attack type you have chosen
2. Any one key website or research paper link that you found was useful.

**Optional Exercise:** You can analyze more than one type of attack.

**PRACTIAL SESSION:**

Step 1:

WannaCry Ransomware Attack (2017)

Step 2:

1- EternalBlue, a zero-day vulnerability in devices, exploit was used.

2- There are different opinions. The US and the UK made an announcement regarding that the government of North Korea was responsible with the WannaCry ransomware attack. However, some people argue that it may be related to the North Korea-based Lazarus Group while others believe it may be from another region and the clues in the malware had prepared to blame North Korea on purpose.

3- The attack had an impact over 150 countries and lots of known victims such as FedEx, Honda, Nissan and NHS (UK’s National Health Services) which can be evaluated as a serious situation. The attack was stopped with a discovery of a kill switch by a security researcher within hours. Still, the affected computers remained unusable and encrypted until the ransom payment was made or reverse encryption was done.

4-The affected computers were encrypted and in a state of unusable. Also, emergency rooms and some devices such as magnetic resonance imaging (MRI) was locked.

Step 3:

1- The exploit was stolen and released publicly by an attacker group called Shadow Brokers on a blogging site. Additionally, this attack uses a dropper known as DoublePulsar and that’s why, the malware is not saved to devices’ disk as unencrypted. So, antivirus programs cannot detect it in the system.

2- The attacked could have been prevented by downloading a Microsoft patch, Microsoft Security Bulletin MS17-010 patch, that has been released 2 months ago. It was automatically loaded to Windows 10 systems, but not the Windows XP systems.

3- If companies use only the latest software versions, this will protect them initially. In addition, they should follow the updates to see the changes. All employees should be aware of the importance of security as well as a backup plan just in case to be ready to any of the attacks.

Resources:

<https://www.cloudflare.com/en-gb/learning/security/ransomware/wannacry-ransomware/>

<https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack>