Assignment 1.4

Discuss and present a Security Vulnerabilities and Cyberattacks

2017 - WannaCry ransomware attack

1. Jody Cham
2. Jinn Liong Chin
3. Han Rong Ng
4. Ang Kok Beng

● **What happened?**

In May 2017, a ransomware attack known as WannaCry spread rapidly around the world, affecting over 200,000 computers in over 150 countries.

WannaCry encrypted files on infected computers, making them inaccessible to users, and demanded a ransom payment in Bitcoin to decrypt the files.

● What is the effect?

WannaCry had a significant impact on a wide range of organizations, including hospitals, government agencies, and businesses.

Many organizations were forced to pay the ransom in order to regain access to their data.

The attack also caused significant financial losses and disruptions to operations.

● **How it did happen?**

•WannaCry exploited a vulnerability in the Microsoft Windows operating system called EternalBlue.

•EternalBlue was a known vulnerability that Microsoft had released a patch for, but many organizations had not installed the patch.

•WannaCry spread rapidly through networks by exploiting the EternalBlue vulnerability

● **How did they solve the problem?**

•A security researcher discovered a "kill switch" that could be used to stop the WannaCry ransomware from spreading.

•This kill switch was activated, which helped to contain the spread of the attack.

•Organizations also took steps to patch the EternalBlue vulnerability and improve their

● **How to prevent a similar attack?**

•Keep your operating system and software up to date with the latest security patches.

•Use strong passwords and enable multi-factor authentication.

•Be careful about what emails you open and what attachments you download.

•Have a backup plan in place in case your data is encrypted by a ransomware attack.