Instructions

Build an attack case study report using this template. If you need help, refer to the instructional video.

There are five content slides plus a title slide in this template. You can receive up to 20 points for each content slide. You need 80 points to pass this assignment.

For your best chance of success, pick an attack or breach with enough information and data so that you will be able to report the required information.

Replace the red text on each slide with your information and change the text color to black or white, depending on the background. You can change the font size, if needed.

When your report is complete, delete this slide and save your file as a PDF to submit for review.

Case Study

WannaCry Ransomware Attack Case Study

An In-Depth Analysis

Attack Category: Ransomeware

Description:-

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. It typically spreads through phishing emails or exploiting vulnerabilities in software.

Statistic:-

According to the X-Force Threat Intelligence Index 2023, ransomware attacks accounted for 23% of all cyber incidents in the past year.

Company Description and Breach Summary

Various organizations worldwide, including the UK’s National Health Service (NHS), Telefónica, FedEx, and Deutsche Bahn.

In May 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries. The ransomware exploited a vulnerability in Windows operating systems, encrypting files and demanding Bitcoin payments for decryption keys.

Timeline

1

Before the Attack:
March 2017: Microsoft releases a security update to patch the vulnerability exploited by WannaCry.

2

During the Attack:
May 12, 2017: WannaCry begins spreading rapidly across the globe.

3

During the Attack:
May 13, 2017: A security researcher activates a “kill switch” that slows the spread of the ransomware.

4

After the Attack:
Ongoing: Organizations work to recover from the attack and implement stronger security measures.

Vulnerabilities

Overall Vulnerability:
The primary vulnerability was the unpatched Windows systems that were exploited by the ransomware.

Vulnerability 1

Lack of timely software updates and patches.

Vulnerability 2

Inadequate network segmentation.

Vulnerability 3

Insufficient user awareness and training on phishing attacks.

Vulnerability 4

Weak backup and recovery processes.

Costs and Prevention

Costs

- Financial Costs: Estimated damages exceeded $4 billion globally.
- Operational Costs: Significant disruptions in healthcare services, logistics, and other sectors.
- Reputational Costs: Loss of trust and credibility for affected organizations.

Prevention

- Incident Response Plan: Develop and regularly update an incident response plan.
- Regular Software Updates: Ensure all systems are up-to-date with the latest security patches.
- User Training: Conduct regular training sessions on recognizing phishing emails and other social engineering attacks.
- Network Segmentation: Implement network segmentation to limit the spread of malware.
- Regular Backups: Maintain regular backups of critical data and ensure they are stored securely.