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

Marriott International Data Breach(2018)

Attack Category:
Name of category

Category: Data Breach

Type: The attack involved unauthorized access to Marriott's Starwood guest reservation database.

Statistics:The breach exposed personal information of approximately 383 million guests, including passport numbers and payment card information.
The hospitality industry, including hotels, has seen a rise in cyberattacks due to its handling of sensitive guest data. According to IBM, in 2018, 15% of all reported data breaches involved the hospitality sector.

Company Description and Breach Summary

Company: Marriott International

•**Incident Summary**:In 2018, Marriott discovered that hackers had gained unauthorized access to their Starwood guest reservation database, starting as far back as 2014.

•The breach exposed sensitive information, including names, phone numbers, passport numbers, email addresses, and payment details.

•The breach affected approximately 383 million guests worldwide.

Timeline

1. **2014**: Attackers initially gained access to Starwood’s network through a vulnerability.
2. **2016**: Marriott acquired Starwood, unaware of the ongoing breach.
3. **September 8, 2018**: Marriott's security tools detected an unauthorized access attempt.
4. **November 19, 2018**: Marriott confirmed that a breach had occurred.
5. **November 30, 2018**: Marriott publicly disclose the breach.
6. **July 9, 2019**: UK’s Information Commissioner’s Office (ICO) fined Marriott £18.4 million (initially £99 million) under GDPR.

Vulnerabilities

Vulnerability 1

Unpatched System: Starwood's IT systems had vulnerabilities that were exploited by hackers to gain initial access.

Vulnerability 2

Weak Control access: Inadequate internal security allowed attackers to maintain long-term access to the reservation database without detection.

Vulnerability 3

Lack of Encryption: Sensitive data, like passport numbers, were not properly encrypted, making it easier for attackers to steal.

Vulnerability 4

Delayed Detection: The breach continued undetected for four years due to weak monitoring and detection capabilities.

Costs and Prevention

Costs

- Marriott faced fines totaling **£18.4 million** from the UK's ICO for violating GDPR.
- The company also incurred legal fees, reputational damage, and compensation for affected guests.
- Overall, the breach could have cost Marriott up to **$72 million**.

Prevention

- **Stronger Access Controls**: Implement strict access policies and multi-factor authentication for accessing sensitive systems.
- **Data Encryption**: Ensure that all sensitive data, including passport numbers and credit card information, is fully encrypted.
- **Vulnerability Management**: Regularly patch and update IT systems to address known security vulnerabilities.