The Marriott Data Breach

A Case Study Unveiling a Major Hospitality Security Lapse

By Chua Lai Chwang
of NTU CE7
on 21 Jun 2024

In late 2018, the hospitality industry was rocked by a massive data breach at Marriott International. This presentation will delve into the details of this cyberattack, exploring how it happened, the impact it had, and the steps we can take to prevent similar incidents in the future.

What Happened?

- Breach occurred in 2014, affecting Starwood guests
- The guest reservation database was compromised
- Personal information of millions exposed – such as names, addresses, birth dates, gender, passport numbers, credit cards info including that of Starwood Preferred Guests
- Not discovered until 2018 by an internal security tool - likely a network monitoring tool on suspicious activities

The attack began in 2014, targeting the guest reservation system of Starwood Hotels, which Marriott had acquired earlier in 2016. Hackers infiltrated the system and accessed the personal information of millions of guests. This sensitive data remained exposed for four years until an internal security tool at Marriott finally identified the breach on 8 September 2018 – likely an internal security monitor that flagged suspicious access attempts.

Impact of the Breach

- Financial costs estimated at around US$28 million for investigation and remediation in 2018 alone
- Over 300-500 million guest records compromised - one of the largest data breaches ever
- Potential for identity theft and financial fraud
- Loss of customer trust and brand reputation
- Legal repercussions of class-action lawsuits and financial penalties from regulatory bodies - e.g., GDPR fines of up to around US$123 million

The scale of the Marriott data breach was staggering. Over 300-500 million guest records were compromised, making it one of the biggest data breaches ever reported. This exposed a vast amount of personal information, putting millions at risk of identity theft and financial fraud. The breach also significantly damaged Marriott's brand reputation and resulted in hefty fines from regulatory bodies enforcing data protection laws like the GDPR (General Data Protection Regulation).

How Did It Happen?

- Initial attack methods remain unclear - possibly malware or compromised credentials
- Legacy systems from Starwood lacked proper security measures
- Delayed detection due to inadequate monitoring

This incident also showed the importance of proper, full due diligence during mergers and acquisitions.

While the exact methods used by the attackers haven't been publicly disclosed, it's believed they could have involved malware or compromised employee credentials. The breach highlights the vulnerabilities of legacy systems. Starwood's guest reservation system, integrated into Marriott's network, may not have had the necessary security measures in place. Additionally, inadequate monitoring allowed the attackers to remain undetected for an extended period.

Resolving the Problem

- Public disclosure of the breach in November 2018
- Investigation by forensic specialists and law enforcement
- Offering credit monitoring and fraud protection services to affected guests
- Implementing stronger security measures - system upgrades, data encryption

Marriott publicly disclosed the data breach in November 2018. They launched an investigation alongside law enforcement and forensic specialists. To mitigate the impact on guests, Marriott offered credit monitoring and fraud protection services. The company also focused on strengthening its security posture by upgrading systems, implementing data encryption, and likely improving internal security protocols.

Preventing Similar Breaches

- Regularly update and patch systems
- Implement robust security protocols - e.g., multi-factor authentication
- Educate employees on cybersecurity best practices
- Continuous monitoring of systems for suspicious activity and vulnerability management
- Have a data breach response plan in place

Several steps can be taken to prevent similar cyberattacks. Regularly updating and patching systems addresses potential vulnerabilities exploited by hackers. Implementing strong security protocols like multi-factor authentication adds an extra layer of protection. Educating staff on cybersecurity best practices, such as password hygiene and phishing awareness, can significantly reduce the risk of human error. Continuous monitoring of systems for suspicious activity and having a well-defined data breach response plan in place allows for faster detection and mitigation of security incidents