Introduction

Marriott hotels experienced what is commonly known as every hotel's worst nightmare in 2018. The Marriott hotels security breach led to hundreds of millions of people having their credit card and passport numbers stolen; not only was this security breach detrimental to the customers that were affected, but also for the reputation of Marriott hotels themselves, as the breach had occurred four years before it was discovered.

Background

The issues for Marriott began when the company bought out Starwood hotels in 2016. When acquired by Marriott, Starwood was still using legacy IT infrastructure, granting them various security vulnerabilities. Starwood was already known for having an insecure reservation system, and Marriott wasn't ready to supply its new hotels with its own reservation system, causing Marriott to rely on Starwood's old, vulnerable reservation system, already heavily infected with malware. The system was found to be infected with Remote Access Trojan (RAT) software along with Mimikatz, a password sniffing tool, the malware is mostly believed to have possibly been downloaded from a phishing email.

Repercussions

The consequences of the security breach were terrible for customers and the business alike. Monetarily, Marriott has paid 3 million dollars after insurance was applied from the accident, however, most of the hotel's current customers had their passport and credit card information compromised. However, the underlying issue of the breach is still being speculated. With Marriott being the largest hotel room provider for the U.S. government and military there is

a possibility that the attack could have been a part of a Chinese effort to create a pool of information on American government and military officials' information. Acquiring the passport numbers of unsuspecting guests could allow for the cybercriminals to track the victim's travel habits. Multiple lawsuits were filed against Marriott, attempting to hold the company accountable for its continuous failures to properly inspect Starwood's IT software. Marriott also agreed to pay for passport replacements for the victims.

Possible Mitigation strategies

Because of Starwood's extremely poor security culture, most simple mitigation strategies could have prevented the data breach. For example, Starwood could have done more to educate their employees on proper cybersecurity hygiene, since it's believed that the malware that caused the breach was likely downloaded from a phishing email. Anti-virus software could have also been used to detect and deter trojans from the reservation system. Anti-virus software may have also been able to alert employees to possible suspicious emails containing the malware. It was also discovered that although the credit card numbers on the server were encrypted, the encryption keys were stored on the same server, allowing them to be easily discoverable by the criminals. Finally, by using network scanning and monitoring tools Marriott could've discovered malware in the already infected reservation system and would've known the software wasn't safe for use by customers yet.

References

Fruhlinger, J. (2020, February 12). *Marriott Data Breach FAQ: How did it happen and what was the impact?* CSO Online. Retrieved March 5, 2023, from https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Marriott Data Breach FAQ: What really happened? - hotel tech report. (n.d.). Retrieved March 5, 2023, from https://hoteltechreport.com/news/marriott-data-breach

Perlroth, N., Tsang, A., & Satariano, A. (2018, November 30). *Marriott hacking exposes data of up to 500 million guests*. The New York Times. Retrieved March 5, 2023, from https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html