Brian Engel

Module 5 Case Study

I am going to discuss the Marriott International data breech that was discovered in 2018. Since it was a massive data breech, there are many independent case studies on it, but you can read Marriotts initial disclosure [here](https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident). This case initially made news because of the sheer size of the breech – personal information from 500 million guests – but later became newsworthy again because it was discovered that the hackers were working for the Chinese government and became an issue of cyber espionage and national security.

Marriott had acquired Starwood in 2016, and unknown to either party the Starwood reservation system was already compromised back in 2014. Marriott still hadn’t integrated Starwood’s reservation system into its own at the time the breech was discovered in 2018. Marriott first became aware that they’d been hacked when a security tool flagged an unusual database query. The database query was made by a user with administrator privileges, but analysis quickly revealed that the person to whom that account was assigned was not the one who made the query; someone else had managed to take control of the account. Investigators began scouring the system for clues and discovered a Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos in system memory. Together, these two tools could have given the attackers control of the administrator account. It’s not clear how the RAT was placed onto the Starwood server, but such Trojans are often downloaded from phishing emails, and it’s reasonable to guess that might’ve been the case here (Fruhlinger, 2020). Marriott was targeted because they are the top hotel provider for the US government and military. The data they stole could have easily been used for identity theft and credit card fraud, but never was. The Chinese government was more interested in tracking government and military personnel as they had gained access to passport numbers.

The immediate threat in this case is unauthorized access to customers’ sensitive information, including credit card details and passport numbers. If the threat is unresolved, it would mean continued access to this information. One thing to consider in this case is just because the information hasn’t been used for traditional criminal purposes, doesn’t mean it can’t happen in the future. The data that was stolen is most likely stored somewhere, and can still be sold off, or even more ironically hacked by other parties.

To help prevent an attack like this, multifactor authentication could have been used to keep a tight control on sensitive systems, along with the principle of least privilege. Training employees to not fall for phishing emails is another simple thing that would help. Some employees will fall for phishing scams no matter how much training they receive though, and if a harmful program is attached to the system there should be a scan to detect it. There is no way it should be in a system for 4 years. When Marriott initially took over Starwood, they laid off the IT department. While this department was obviously not very good because the system had been compromised for 2 years at the time of acquisition, they at least had so insight into how the system was supposed to work and could have possibly caught the breech a little earlier.

With the use of Triple A (Authentication, Authorization, and Accounting) and Defense in Depth most attacks can be stopped or at least cut short. Authentication techniques such as multifactor authentication help to verify the user attempting to log in. By using the principle of least privilege in Authorization, even if an attacker gains access, the damage won’t be as bad as if they had access to everything. If something does go wrong, Accounting through user activity logs help to catch suspicious activity and trace it back to the flaw in the system that let the bad actor in. Defense in Depth ensures that there are multiple security measures in place and the software does not rely on one catch-all layer. This way the holes in the layers don’t line up and all the threats are caught.

Fruhlinger, J. (2020, February 12). Marriott data breach FAQ: How did it happen and what was the impact? CSO Online. https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html