DB CyberTech

Whitepaper

The Marriott Breach – A Classic Insider Threat that Behavioral Analysis Immediately Identifies

Background of Marriott Data Breach

On November 30, 2018 Marriott disclosed that the reservation system for their subsidiary Starwood Hotels & Resorts Worldwide had been breached. Marriott stated the breach had actually begun in 2014 and was only recently been detected. That's a horrendously long dwell time by anyone's standards.

The Marriott structured data store breach resulted in the theft of highly sensitive personal information of approximately 500 million guests – including names, mailing addresses, phone numbers, email addresses, passport numbers, and, in some cases, encrypted payment card information. While Marriott is a U.S corporation many of their guests over this period will certainly have been citizens of the European Union (EU). As such, the breach falls under EU GDPR legislation. This means Marriott could face a fine of up to 4% of its annual revenue which in this case would be $900M.

According to *The Guardian*, "In the past two years many companies were over-concerned to comply with GDPR on paper, ignoring practical security requirements due to limited budget and resources. Management is often satisfied with a formalistic approach to compliance, ignoring the practical side of cyber security and privacy".

Marriott acquired Starwood in 2016. However, in 2015 Starwood had reported a breach of their point-of-sale network resulting in the theft of payment-card information. Clearly this 2015 security incident is not directly related to the loss of records of 500 million customers in 2018. However, the 2015 security incident does emphasize that their security perimeter was vulnerable enabling internal systems to be attacked.

According to Marriott the stolen personal information was staged to a compromised internal server where the data was then encrypted. It's likely the attackers encrypted the data to obfuscate it so that Data Loss Prevention (DLP) systems could not identify the stolen information as it exited the Marriott network.

Classic Insider Threat

The Marriott breach represents an example of a classic insider threat. That may not appear intuitive but it's the correct way to assess it. When we speak of the insider threat various connotations immediately come to mind. Perhaps you think of whistleblowers trying to damage an organization by leaking proprietary information or maybe employees seeking to profit through persistent industrial espionage. While these examples certainly represent a credible danger, there's a category of risk that includes a much more significant threat such as what we likely have in the Marriott

breach — external attackers who have breached the perimeter and appear as legitimate insiders.

Existing perimeter security mechanisms have proven time and again to be an ineffective countermeasure against the insider threat. Hackers have evolved their techniques to the point where the typical enterprise security perimeter has become extremely porous. Traditional perimeter security rely on white lists / black lists and signature files that are continuously updated to address the latest threats seen in the wild. These techniques aren't oriented towards detecting and preventing potentially harmful activities performed by (allegedly) trusted individuals and systems. Perimeter security is also positioned in the wrong location on network to monitor for insider threats. Further, organizations generally assume that authorized corporate users should be trusted. In today's reality that assumption can lead to devastating results.

The Marriott breach once again serves to emphasize that mission critical organization information resides in structured data stores. To effectively defend this data organizations are rapidly adopting a new security paradigm based on machine learning and behavior analysis.

DB CyberTech's Approach to Insider Threats

DB CyberTech's insider threat solution generates a behavioral model of structured data activities observed on the network. This model is an accurate representation of normal SQL activities. The model is then used to immediately detect new behavioral patterns not previously seen. Insider threats immediately stand out due to their unusual activity. There's a universal truth witnessed in every cyber attack – attack behavior never appears normal activity.

DB CyberTech's field proven solution detects a wide array of behavioral changes, whether they are major (such as a significant surge in accesses of a specific table) or minute (such as an authorized user querying a table they've not accessed previously). In addition, DB CyberTech offers advanced security solutions that continuously monitor for GDPR compliance and protect personal data on structured data stores.

Summary

Insider threats, such as those associated with the Marriott breach, are considered one of the top concerns in IT security due to the devastating impact on business, reputation, loss of sensitive data, and significant fines. Security solutions that rely on white lists / black lists and signature files fall far short in their attempt to mitigate this threat. Machine learning and behavioral analysis are uniquely suited to immediately identifying anomalies that indicate an insider threat before any data is lost.