The Capital One Data Breach of 2019: A Detailed Examination

Eric Mung'aũ Preston

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Mr. Malik A. Gladden

1/21/23

The Capital One Data Breach of 2019: A Detailed Examination

Abstract

Within the industry of cybersecurity, a primary area of focus for research is data breaches. They can provide valuable information not only for learning new mitigation strategies and developing policies but also valuable knowledge that companies can use to protect themselves in the future. This paper will go into detail on the Capital One data breach of 2019. The areas of focus will be inspecting vulnerabilities, the threats to those vulnerabilities, overall impact, and potential mitigation strategies to minimize or prevent the breach.

Introduction

In 2019, a significant data breach occurred at Capital One. According to Neto et al. (2020), the breach of Capital One was "the result of an unauthorized access to their cloud-based servers hosted at the Amazon Web Service (AWS)" and the cybercriminal went unnoticed from March 22nd, until July 19th. In September, Capital One put out a statement about what happened, and that the FBI caught the criminal. That person was Paige A. Thompson and is serving 25 years in prison for this breach (Neto et al., 2020). So, to better understand this breach, what needs to be addressed is the vulnerabilities that allowed this to take place.

Vulnerabilities

Vulnerabilities are often found at every level from the system model to the management of the Information Security department. Neto et al. (2020), noted that one of the vulnerabilities that led to the breach was a "configuration failure in the Web Application Firewall (WAF) solution employed by Capital One." Another vulnerability was the lack of enforcement of safeguards by the upper management. Cyber staff noted "Routine cybersecurity measures to help protect the company sometimes fell by the wayside" (Neto et al., 2020). Furthermore, when the

hacker queried the AWS metadata service, they received an Identity and Access Management (IAM) role containing a token for access (Khan et al., 2022). While these vulnerabilities gave easy access to the servers, the criminal had other tools to exploit vulnerabilities.

Threats Exploiting the Vulnerabilities

The lack of proper configuration for Capital One's WAF allowed for a Server-Side Request Forgery (SSRF) attack to bypass the security of the servers entirely. The hacker also used the Tor Network and the VPN IPredator to mask themselves from being detected (Neto et al., 2020). According to Khan et al., (2022), ModSecurity, the open-source firewall Capital One was using, is unable to detect VPNs and if not properly configured, can lead to error-prone messages. The hacker also took advantage of instance roles, which are a flaw in Capital One's process model where the environment trusts the "cloud's security." These threats along with the vulnerabilities of the system, caused a substantial impact on Capital One, AWS, and the customers involved.

Impact of the Breach

In terms of impact, roughly 106 million accounts were compromised combining the United States and Canada (Capital One, 2019). Some of the examples of information were consumer and small business data, credit card applications with personal information, and status data on finances. Additionally, in Capital One's 2019 report, it was noted that the cybercriminal gathered "About 140,000 Social Security numbers of our credit card customers" and "About 80,000 linked bank account numbers of our secured credit card customers." However, while the breach was patched quickly after being discovered, a $190 million Class Action Settlement was put in place against Capital One to pay for the potential and actual damages (Capital One Data Breach – Home, n.d.).

Mitigation Strategies

Despite the scale of this breach, several potential strategies could have been adopted to mitigate or prevent it. One strategy would be the monitoring and auditing of AWS administrative accounts to maintain confidentiality (Neto et al., 2020). An example of this strategy was Security Groups, which could ensure necessary access and auditing of user identity. For the operational level, Khan et al. (2022) recommended security practices such as the principle of least privilege and defense-in-depth to mitigate data access and enforce restriction.

Conclusion

The Capital One data breach of 2019 was one of many breaches that provided valuable information on how companies should approach security. Vulnerabilities such as poorly configured firewalls and a few boundaries on access roles allow cybercriminals to easily breach systems that affect millions of people. Using open-source software is also a bad practice that creates more issues. However, strategies such as Security Groups and the principle of least privilege can reduce the chance of potential breaches. As businesses integrate technology as the foundation for their structure, more emphasis needs to be placed on securing all access points to information as much as possible to mitigate or prevent large data breaches from occurring in the future.

References

"Capital One Data Breach - Home." Www.capitalonesettlement.com, n.d., www.capitalonesettlement.com/en. Accessed 20 Jan. 2024.

Capital One. "2019 Capital One Cyber Incident | What Happened." Capital One, 23 Sept. 2019, www.capitalone.com/digital/facts2019/. Accessed 20 Jan. 2024.

Khan, Shaharyar, et al. "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned." *ACM Transactions on Privacy and Security*, vol. 26, no. 1, 7 Nov. 2022, https://doi.org/10.1145/3546068. Accessed 20 Jan. 2024.

Novaes Neto, Nelson, et al. "A Case Study of the Capital One Data Breach." *Papers.ssrn.com*, 1 Jan. 2020, papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567. Accessed 20 Jan. 2024.