**Case Study: Triple A and Defense in Depth**

Justin Starr

Department of STEM

CS 405 – Secure Coding

Professor Mike Alesso

August 4, 2024

**Case Study: Triple A and Defense in Depth**

The following is a short analysis of the case study that was conducted on the Capital One data breach that occurred on July 19, 2019 (Neto et al., 2024). The reason why this case study is significant was because, at the time of this case study, Capital One was the fifth-largest consumer bank in the U.S. and the eighth-largest bank overall. The security breach that occurred reportedly affected approximately 6 million consumers in Canada and 100 million consumers in the U.S., with the theft of personally identifiable information including names, addresses and zip codes, postal codes, phone numbers, email addresses, dates of birth, and income (Neto et al., 2024). The following analysis will discuss the type of security and data breach, why the company was a target, the immediate and potential threats, which policy or policies will help prevent this type of attack, and a summary of the case by explaining the role of best practices, Triple-A, and Defense in Depth in preventing future attacks.

The breach that occurred was a combination of a security and a data breach. A former Amazon worker, Paige Thompson, created a software tool that would scan and identify servers that were hosted in the Amazon Web Service (AWS) cloud computing infrastructure that had misconfigured firewalls enabling her to execute commands remotely to gain access to the servers (Neto et al., 2024). Once access had been gained, Thompson was able to execute commands that enabled her to locate folders or buckets of data and then copy the data from the Capital One storage space. Capitol One was not explicitly the target, however, because they were utilizing AWS’s cloud computing infrastructure, and their storage happened to be on one of the servers where the firewall was misconfigured, they inadvertently became a target of the attack. The reason why any of the AWS servers would be a target of value is because of the type of information the servers were storing; personally identifiable information. If a user were to gain access to this type of information or data, they are a target because this information can be sold to identity thieves who can then use this data to wreak havoc on consumers, causing millions of dollars of damage.

In this case, the immediate threat was that a user was able to gain unauthorized access to a vulnerable server because of a Server-Side Request Forgery (SSRF) attack, which was made possible because of a configuration failure in the Web Application Firewall (WAF), which was used by Capitol One (Neto et al., 2024). The SSRF attack is designed to trick a server into executing commands for a remote user, where the user is then able to treat the server as a proxy for the user's requests, enabling access to end-points that are not public (Neto et al., 2024). If the vulnerability were to go unresolved, the remote user would be able to continually gain access to not only Capitol One’s data that is stored on the server but also any other company who also stores data on the server. It was reported that not only did Thompson gain access to Capitol One’s data that was stored on the server, but she had gained unauthorized access to 30 different companies’ data that had been stored on AWS servers (Neto et al., 2024). The longer the vulnerability goes undetected or unresolved, the more data that is likely to be exposed and likely sold to individuals who would likely use the information fraudulently.

It was determined that a number of policies could have been enforced to help prevent this vulnerability from occurring. The attacker was able to use TOR network to hide the origin of the attack. At the firewall level, the IP addresses from TOR network exit nodes and malicious proxy server should have been blocked, and if successful access occurs, the system should have alerted on IDS/IPS the successful access from the malicious IP addresses (Neto et al., 2024). SSRF attacks could be mitigated by a well-configured Web Application Firewall (WAF), and with the use of preventative controls such as periodic vulnerability scanners. Also, to mitigate the initial access of the system, monitors and audits should have been in place to analyze the use of administrative controls/accounts. To prevent the execution of commands and the discovery of data (the listing of buckets in AWS S3), tracking should have been in place to monitor commands on the AWS account. To prevent the data from being exfiltrated, outbound traffic monitoring should have been implemented (Neto et al., 2024). According to Neto et al. (2024), while there were numerous cyber security controls that failed, however, there were two primary security controls that failed during two relevant steps that existed in the attack’s chain of events. “The existence of technical controls to monitor and audit the use of administrative accounts and to monitor outbound traffic could have prevented the privilege escalation and the data exfiltration” (Neto et al., 2024).

The role of best practices, Triple-A, and defense in depth in preventing future attacks is paramount. Triple A refers to Authentication, Authorization, and Accounting. Authentication is the first step in the Triple-A security process, and it is the way a network or application identifies a user and that that user is who they say they are (Mylonas, 2018). A user will attempt to authenticate by providing credentials, which are then used to compare against existing credentials stored in a database. If the user's credentials match existing credentials, the user is authenticated, where they then must gain authorization, otherwise, the user is denied access to the network or application (Mylonas, 2018). Authorization is the process of enforcing established policies for each user. These policies determine what resources, services, or quality of activities a user is allowed to use, and they assemble the set of attributes that essentially describe what the user is authorized to do (Mylonas, 2018). Accounting means to keep track of what a user is doing. It means keeping track of who the user is, what resources they are consuming, and when they are consuming them, and also if the user executes or issues commands, keeping track of the commands that are issued (Mylonas, 2018). As determined by the case study, one of the major concerns of the vulnerability was that there were insufficient accounting measures in place to mitigate the attack. It is essential that Triple-A practices at each stage are enforced to help prevent vulnerable attacks.

Defense-in-depth is a security strategy, which employs at various layers, multiple security tools whose aim is to protect a network or application from potential vulnerabilities. The idea of it being layered means that if one security measure fails, there are additional security measures in place to help mitigate vulnerabilities (Fruhlinger, 2022). In the case of Capital One, had they implemented a better layered defense, including the use of Triple-A defense, they would likely have been able to detect the intrusion, and possibly take steps to prevent the data breach from occurring.

**References**

Fruhlinger, J. (2022, July 28). *Defense in depth explained: Layering tools and processes for*

*better security*. CSO. <https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html>

Mylonas, L. (2018, November 27). *What is AAA security? An introduction to authentication,*

*authorisation and accounting* Codebots. <https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting>

Neto, N., Madnick, S., Paula, M., & Borges, N. (2020). *A Case Study of the Capital One Data*

*Breach.* Cybersecurity Interdisciplinary Systems Laboratory, Massachusetts Institute of Technology. <https://web.mit.edu/smadnick/www/wp/2020-07.pdf>