Ryan G. Cooper

Professor Conlan

CS-405 Module 5 Assignment One

June 9th, 2024

**Case Study**

In an era where data is a critical asset, the protection of personal and financial information is critical. The Equifax data breach, discovered on July 29, 2017, and publicly disclosed on September 7, 2017, is an example of the severe consequences of inadequate cybersecurity measures. The breach made headlines due to its massive scale and the sensitivity of the compromised information. Attackers exploited a vulnerability in the Apache Struts web application framework, which Equifax had failed to patch despite it being publicly known and fixable. Equifax was attacked because they are a credit report company and store personal information about credit history. This allowed unauthorized access to sensitive data, including Social Security numbers, birth dates, addresses, and, in some cases, driver's license and credit card numbers, affecting approximately 148 million individuals. The immediate threats posed by this breach included identity theft and financial fraud, while unresolved vulnerabilities could lead to ongoing attacks and further damage to the effected users like identify thief.

To prevent such breaches, developers should implement regular security audits, timely application of patches, robust input validation, and multi-factor authentication. Security should be at the forefront of development and maintenance. This is because attacks like these are preventable and have long term impacts on the effected users and the brand of the Equifax. Policies like regular security training, strict patch management, and access control are crucial. Furthermore, employing the Triple A framework—Authentication to ensure only authorized access, Authorization to limit permissions based on roles, and Accounting to maintain detailed activity logs—along with a defense-in-depth strategy that layers multiple security measures, can significantly enhance an organization's security posture. The Equifax incident highlights the need for a cybersecurity strategy that integrates these best practices to protect against potential threats and safeguard sensitive information effectively.

**References**

Ontiveros, V. (2021, June 15). Equifax Data Breach. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/equifax-data-breach