UC Data Breach

University of the Cumberlands

Dr. Brian Bertrand

Jacob Jeffers

ISOL 536 – Security Architecture and Design

08/17/2021

**Abstract**

In this final project, I will define a security breach and describe ransomware attacks. I will review the University of California security breach that occurred between the first and second quarters of 2021. I will describe the incident, provide specifics on the incident, describe the impacted data, describe threat modeling techniques that could have assisted in the mitigation of the breach, and explain how the organization could be better postured for future attacks. In addition, I will utilize the APA format and include references when necessary.

**Table of Contents**

Cover Page ………………………………………………………………………………………..1

Abstract …………………………………………………………………………………………...2

Table of Contents …………………………………………………………………………………3

UC Data Breach ……...…………….……………………………………………………………..4

Resources …………………………………………………………………………………………6

**UC Data Breach**

A breach is any incident that occurs when an individual unauthorized gains access to resources, data, or devices (Schoenfield, 2015). Usually, it comes about when an attacker bypasses the security mechanisms that are put into place. In March of 2021, the University of California released a statement that it was the victim of a potential ransomware attack due to an exploit of their file transfer software known as Accellion File Transfer Application (Williams, 2021). However, the attack spanned multiple governmental and higher education agencies which still utilized the software. The software was legacy software and was being phased out into an updated application. A ransomware attack occurs when a file or the file system is compromised, usually through encryption, and the attackers request some payment for their safe return (Fruhlinger, 2020).

In March, before the attack on the University of California and the school systems, Accellion released a statement in January stating that it was aware of the vulnerabilities and was working on a patch release. They notified existing customers of the events. The stolen data included personal information about faculty and students. According to Morgan (2021), the compromised users received an email stating, “Your data has been stolen and will be published.” After becoming aware of the incident, an investigation was conducted into the situation. As a result, the University of California notified the authorities, encouraged the victims to forward suspicious emails, and offered a year of credit monitoring and ID theft protection (Morgan, 2021).

To summarize, a vulnerability was exploited in the legacy software in Accellion’s FTA to obtain personal information from faculty, staff, and students attending the University of California. Authorities were notified, and an investigation was conducted. The investigation revealed that personal information had been compromised, and the details of the exploit were discovered. Some mitigation strategies would be to monitor all third-party software for vulnerabilities and patch regularly constantly.

For a better posture in the future, backups should exist and be protected, networks should be segmented to prevent outsiders from gaining access, remote access should be disabled, when necessary, user accounts should be audited to ensure the principle of least privilege is followed, and MFA authentication should be implemented (Schoenfield, 2015). In addition, organizations should focus on developing risk mitigation strategies and training how to handle certain events like ransomware attacks. These plans and policies give users guidance on how to handle situations.

**References**

Fruhlinger, J. (2020, June 19). *Ransomware explained: How it works and how to remove it*. CSO Online. <https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>.

Morgan, L. (2021, April 30). *IOTW: University of California Schools hit with a ransomware attack*. Cyber Security Hub. <https://www.cshub.com/attacks/articles/iotw-university-of-california-schools-hit-with-ransomware-attack>.

Schoenfield, B. S. E. (2015). *Securing Systems: Applied Security Architecture and Threat Models*. CRC Press.

Williams, J. (2021, April 3). *University of CALIFORNIA victim of a ransomware attack*. TheHill. <https://thehill.com/policy/cybersecurity/546335-university-of-california-victim-of-ransomware-attack>.