Final Project

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for NTS405, taught by Professor Aaron Jones.

Abstract

The purpose of this paper is to cover a wargame (a theoretical simulation) in which a corporation suffers a data breach and has to recover.

Final Project

Introduction

At 3:30 AM on Tuesday, August 11th 2020, Company Inc., a corporation that provides a video and music streaming services on their website, suffered a data breach. An unknown party had gained admin credentials and remotely accessed the corporation's backup of user data, allowing them to steal unencrypted user data. It took three hours before, at 6:40 AM, system administrator Neil Hendricks detected the intrusion after sitting down at their workstation in the morning and disabled the attacker's credentials. President of Company Inc., Victor Loserson, after a few hours of trepidation, submitted the details of the attack to law enforcement and began readying a public statement to the company's base of customers. He directed the head of security, Deborah Cyberli, to uncover how the attack was done, if they are still in danger, and what to do next.

The Attack

Looking through the logs, it was revealed that the intruder utilized the credentials of one Seth Snaketongue, a junior system administrator working for the company. He was questioned and revealed that he had not only utilized the same password on every site he registered on, but it was "password123". Upon further investigation, one of his accounts was discovered to have been subject to a breach, his username and password having been posted publicly and sold a year ago.

Cyberli resisted the urge to slap Snaketongue and settled on simply demoting him to a janitorial position (which he quickly left) and set about tracing the intruder's footsteps through their network. She discovered that after gaining access to Snaketongue's credentials, they logged in on the website and managed to remotely access a client on their network. Afterwards,

they tested their credentials until they were able to gain access to Company Inc.'s local database where they stored user information.

Cyberli then contacted Becky Blockhead, Company Inc.'s sole database administrator. Blockhead revealed that their entire database was not only accessible to anyone with junior-level security credentials, but also that she was storing all of their user data in plain text, including passwords, which were not hashed. When asked why, she said that although she was instructed to encrypt the data, her supervisor, Larry Lazybones never checked up on her after giving the initial order. She also said that "all this security stuff" confused her greatly and asked if perhaps the data would be more secure outside of an SQL server and in an Excel sheet.

After firing Blockhead, Cyberli carefully analyzed the logs and realized that, thankfully, the intruder only had access to the client they remotely accessed and the database before they were cut off. She set about securing their systems on the level of user credentials: all users now had to make new passwords every financial quarter, the system requiring a 12-character minimum for each password with upper and lowercase characters along with numbers and symbols. She went over permissions and ensured via a plethora of GPOs (group policy object) that low-level accounts only had the bare necessities of permissions, with the greater privileges being restricted to higher level accounts.

As for securing the credentials, Cyberli went about securing the database. She hired a new database administrator who was able to portray a level of competence and experience in securing databases via encryption, allowing for the information stored to be held in a safer state than before. Additionally, passwords were placed in hashes so even if the database was accessed, the passwords would still likely be safe.

Aftermath

President Loserson released a public statement the next day detailing the attack to customers and news outlets. Claiming that unprotected user data had been available to the attacker for a total of three uninterrupted hours caused a stir amongst the userbase of the corporation, causing a brief public outcry against the company on social media. After the backlash began to fade, Loserson called a meeting of company executives and discussed how to handle the matter further. They decided to upgrade their security beyond what it was before (as seen with Cyberli), and release another public statement apologizing for the security breach and promising to do better. Additionally, they briefly allowed for a month-long discount on their premium service for users as a way to calm backlash and satisfy disgruntled customers.

Loserson contacted law enforcement and enquired as to the state of their investigation. After letting their investigators go over the company's logs and data, forensics experts determined that the attacker, although utilizing a VPN (virtual private network), was likely located in the Russian Federation, meaning that while they could report the breach and document it to possibly compare to other attacks and build a case on the suspect, there was little they could do at the moment. Frustrated, Loserson asked them if they could investigate further or perhaps do "more digging" to uncover anything else but was refused, being told that the investigators had done all that they could and that nothing more could be done.

Neil Hendricks was awarded the "Employee of the Month" award for discovering the attack and acting quickly to take away the compromised credentials, later receiving a bonus and promotion a few months down the line. Cyberli advised Loserson to hire a cybersecurity consultant to consider the security of their system and see if it compared to modern standards, as well as asking him to hire penetration testers to test security down the road. Loserson accepted

both proposals, the consultant he hired advising him to employ a multi-factor authentication system in their security infrastructure, which was later done. Next, penetration testers revealed further holes in both their cybersecurity and physical security, which would be ironed out in the coming years. Although they would never find the culprit behind the attack, Company Inc.'s security upgrades ensured that such a breach would likely not occur again for some time.

References

No references were utilized in this document.