Assignment 1-1

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for NTS350, taught by Professor Michael Vasquez.

Abstract

The purpose of this paper is to analyze a recent network intrusion (the Radio.com breach) and relate it to the topic of detecting and responding to intrusions.

Assignment 1-1

Summary

In September 2019, the corporation Entercom detected a data breach while investigating an attack to one of their systems. Upon later examination, they had confirmed that a large degree of private information was accessed by an unauthorized individual. They determined that the individual had accessed a third-party cloud hosting service where Entercom sotred data regarding users of their website "Radio.com." It was after further investigation that they discovered on August 4th of 2019, a hacker had accessed to—for a period of three hours—a host of private information, such as the names, usernames, and passwords of website users.

Entercom implemented a variety of measures after the breach to prevent similar incidents in the future, such as multifactor authentication, better password policies, and data security training for staff. They also advised users to change their passwords for their Radio.com accounts (along with other accounts using the same password).

Analysis

It is worth noting that password hashes were not accessed during the attack, the passwords themselves were. This implies that the any credentials accessed in the breach were being stored in plain text. This has not been verified (security practitioners BleepingComputer reached out to an Entercom spokesperson to verify if this was the case but did not receive any response) (Cyber Security News, 2020). This would underscore a general lack of thought as it relates to the security of Entercom's customer data and imply that similar aspects of their security are also lacking in depth, strategy, and/or adherence to contemporary standards.

Detecting and Responding to Intrusions

It is likely for security reasons that Entercom did not detail the exact specifics on how the attack was conducted or the third-party cloud hosting service accessed. Regardless, accurate speculation regarding Entercom's detection and response to the intrusion can still be conducted from what has been made public about the breach. It is more likely than not that Entercom has some sort of IDS (Intrusion Detection System). This system obviously failed to alert Entercom of the breach when it happened, evidenced by the corporation discovering it a month later while investigating a likely unrelated cyberattack. Furthermore, if they have an IPS (Intrusion Prevention system), it too failed to impede the intruder from accessing their system. Additionally, security staff may not have been practicing NSM (Network Security Monitoring), as since the intrusion went undetected for a month, neither hardware nor security specialist was aware of the network traffic that would have likely communicated an intrusion. CM (Continuous Monitoring) was not likely put into effect, as staff should have realized the vulnerability of their hosting service being accessible through their network along with other weaknesses. The passwords were also obviously not in hashes since they were obtained directly in their pure form, indicating a lack of care and thought as it related to the database backup files they were stored in (as stated earlier, the fact that the passwords were not in hash form implies they were, along with other sensitive customer data, being held in plain text).

Ideally, what would have happened would be that an IDS would have detected and alerted security staff to the intrusion as soon as it occurred, while perhaps an IPS would have impeded or completely stopped the intruder from gaining access to their network. Furthermore, NSM would have been utilized, allowing security staff to detect what exactly the intruder was trying to do upon their attempt to gain access to the network and—assuming if they were

successful—what their goal was once they got in. Meanwhile, CM would have caused system administrators to regularly repair and check their vulnerabilities before the attack occurred, perhaps allowing them to ensure that easy movement to the third-party cloud hosting service they utilized to store data was not able to be so easily accessed. Finally, the customer data that was being held in said third-party service (which were contained in database backup files) would have been protected some way, with passwords held in hashes instead of plain text. Perhaps the files themselves would have been encrypted for further security.

It can easily be concluded from the public release of Entercom regarding their breach that their intrusion detection and prevention systems, their staff monitoring, and their data protection methods are not only behind contemporary standards but weak to the point of endangering millions of their customers. Since the breach was identified a month afterwards, it can easily be reasoned that Entercom had no knowledge of the attack when and as it occurred, and the month of time after the incursion means that customer data could have easily been sold and utilized by malevolent parties to access customer information on not only Radio.com but other sites where the same passwords were used with the same usernames. Entercom can only hope to improve their security to prevent similar accidents in the future, as this attack—as a result of their lack of sufficient protection—seems to have went generally impeded and easily for whoever carried it out.

References

Balaij, N. (2020, March 11). *Radio.com hacked: Hackers accessed Radio.com credentials*. Cyber Security News. https://cybersecuritynews.com/radio-com-hacked/

.