Maame Darko

Old Dominion University

Introduction to Cybersecurity

CYSE 300

May 19, 2023

Research paper #1

Cybersecurity Breach

What is a Breach?

A breach refers to the unauthorized entry, theft, information alteration, copying, transferring, and viewing a sensitive data or confidential information from an organization or an individual by an internal or an external attacker or cybercriminal.

Example of branches are:

- Malware
- Ransomware
- Phishing
- Password hacking
- Business Email Compromise (BEC)

Introduction

In the past decade, there has been a tons of Cybersecurity breaches. But one of the massive ones is, Data Breach at eBay Compromised 145 million Records. Online marketplaces have been incorporated into day-to-day life. However, because of their developed use, digital platforms have become more appealing and easy targets for hackers. In 2014, eBay experienced one such big cybersecurity attack that compromised over 145 million user records. This research paper investigates the eBay data breach, What the cybersecurity vulnerabilities were, what threat(s) exploited the vulnerabilities? What were the repercussions of the incident? and What cybersecurity measures could have been taken to mitigate the consequences or prevent the incident?

Overview \What happened?

Three employees' login information was stolen, allowing hackers to easily access the eBay network and steal customer information such email addresses, phone numbers, names, dates of birth, and physical addresses. eBay discovered the hack in May 2014 and took quick action, including recommending for users to change their passwords. The breach damaged eBay's brand and led to legal and regulatory investigations.

What were the cybersecurity vulnerabilities/threats?

The attackers were able to gain unauthorized access to eBay's network and exploit weak password security mechanisms. They went through the network, gaining access to a database containing confidential information.

- Compromised Employee Credentials: Compromising credential is when unauthorized users take control over an individual's or and organization's confidential information of their account. In the eBay breach, employees' credentials such as usernames and password were stolen which gave them access to the eBay network.
- Phishing: Phishing involves sending a message mostly through emails that include links to give cybercriminals access to the information needed when the victims click on it. In the eBay breach, this was one of the vulnerabilities. Employees were deceived into revealing their login information through spear-phishing.
- Delayed detection of breach: I took their security team a couple weeks to detect the breach. This gave the attackers a lots of time to get the information they needed for any action they wanted to take with it.

What were the repercussions of the incident?

145 million user records were exposed, exposing users to identity theft. This breach affected eBay's reputation, which caused users to not trust the website and the organization. They also had

a financial strain as a result of the spending on investigating the breach, taking corrective measures, and potentially paying legal fees.

What cybersecurity measures could have been taken to mitigate the consequences or prevent the incident?

- Two Factor Authentication: This is basically a method that only grants access to users once they have confirmed their identity through security token or biometric factors. Having two Facto Authentication would have prevented the attackers from accessing their confidential information with just the passwords.
- Having a great incidence report team/ Good incidence plan: The fact that the incident or hack took many weeks to resolve demonstrates how unprepared eBay was when it came to confidential information being leaked. Having a plan for emergencies in any situation could help them resolve difficulties more quickly when they occur.
- Employee Training: Offering cybersecurity awareness training to employees, with a specific emphasis on recognizing and reporting phishing attacks, This could reduce breaches and make them more aware of cybercriminals.

Conclusion

The 2014 eBay data breach is a notable example of a cybersecurity breach that affected 145 million user information. The event disclosed vulnerabilities such compromised employee passwords, phishing attempts, and delayed breach discovery. The consequences included damage to eBay's reputation, financial burden, and the possibility of identity theft for users. Implementing two-factor authentication, developing an effective incident response plan, and offering extensive employee cybersecurity training are critical methods for mitigating such incidents.

REFERENCES

"EBay 2014 Data Breach: With Big Data Comes Big Responsibility." *Skillsire*, 12 July 2020, www.skillsire.com/read-blog/266_ebay-2014-data-breach-with-big-data-comes-big-responsibility.html#:~:text=What%20happened%3F,email%20(reuters.com).

"Top Cyber Breaches of the Last Decade." *Maryville Online*, 26 Jan. 2021, online.maryville.edu/blog/the-top-cyber-security-breaches-of-the-last-decade/.

"Hackers Raid eBay in Historic Breach, Access 145M Records." *CNBC*, 22 May 2014, www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html.