Southern New Hampshire University

CS 405 Secure Coding

Professor Mike Prasad

Student: Tyanna Prince

11/26/2022

**Introduction**

The data breach case I chose for this case study is the Yahoo data breach that took place in 2014. This data breach affected 500 million people and resulted in a lawsuit against Yahoo. During the lawsuit, it was made known that there were multiple data breaches between 2012-2016 with information stolen getting more specific happening between 2013-2016. In 2014 Yahoo’s database was attacked resulting in 500 million peoples account details being stolen. The data breaches were not made public until the year 2018 which is when they were sued for the data breaches. Yahoo ultimately ended up with a 35 million dollar fine for not disclosing the breaches. This is the reason this breach became a popular trend in the news.

**Describe the Breach**

Each data breach that took place had different kinds of data stolen. In 2012, there were two separate hackers that hacked Yahoo but did not steal any information. In 2013, other hackers took records from all Yahoo accounts, which was around 3 billion at the time. These hackers then have access to user emails, calendars, and accounts. In 2014 Yahoo’s database was attacked resulting in 500 million peoples account details being stolen. The hackers could access accounts, passwords, emails, etc. from this hack. The cause of such a catastrophic data breach? A single spear phishing click! It only took one accidental click for the hacker to access Yahoo’s network. The hacker sent emails to Yahoo employees in the hopes that one employee would mistakenly click the link inside the email. According to The United States Department of Justice, “A grand jury in the Northern District of California has indicted four defendants, including two officers of the Russian Federal Security Service (FSB), for computer hacking, economic espionage, and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo’s network and the contents of webmail accounts. The defendants used unauthorized access to Yahoo’s systems to steal information from about at least 500 million Yahoo accounts and then used some of that stolen information to obtain unauthorized access to the contents of accounts at Yahoo, Google, and other webmail providers, including accounts of Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies”.

**Identify the threat(s)**

Data breaches like this can affect the company, it’s affiliates, and most importantly the users. Hackers who gain the users person email, account, calendar, etc. information can easily then access things like credit card info, home and work addresses, phone numbers, and more. The hackers can benefit from this information by using it themselves or selling this information on the black market to gain even more profit. This is the immediate threat from these attacks and if the breach goes unresolved the number of users and information that they can gain access to only grows allowing hackers to steal even more information from users of Yahoo’s affiliates. Such as in the 2014 case where the hackers gained access to the contents of accounts at Yahoo, Google, and other webmail providers, including accounts of Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies. Making this breach one of the nations biggest data breaches of all time.

**What Could a Developer Have Done to Prevent this Breach?**

Yahoo being a big company could have prevented this breach by updating and/or creating a better email filtering service. It’s known that yahoo did not use a third-party service that have specialized tools available to prevent these types of attacks from happening. It seems Yahoo themselves attempted having their own email filtering service and it’s possible that it was not well built for filtering potential threats and phishing scams. According to CNN business, “Yahoo resisted calls for greater funding and efforts to bolster security. Security was pushed back to the back end and the higher-ups within Yahoo commented that “we just had other priorities”. Yahoo could have prevented these attacks if it had made security one of those priorities.

**Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.**

**Authentication**

Authentication policies could have helped in this type of breach. Yahoo didn’t offer things like multi-factor or biometric authentication. If Yahoo had these types of authentications if could have prevented a lot of user information from being stolen. Multi-factor/biometric authentication allows the user to sign on with their password and a code would be sent to an alternate email or phone which would need to be entered before accessing their accounts. Biometric authentication allows users to use their fingerprint for verifying they are the owner of the account they are trying to access. These simple but powerful authentication methods could have been implemented into Yahoo’s sign on process to prevent hackers from gaining access to user accounts without this second form of identification.

**Authorization**

Authorization policies could have helped Yahoo’s systems identify the hacker and lock him out once the employee clicked the link. Authorization would enable Yahoo’s database to determine that the hacker did not have permissions to use the resources and access the files within. Authorization is accompanied by authentication they work hand in hand. Yahoo did not have these policies, or they lacked fully operational security features within its database. Yahoo could have implemented a user + add-in policy which would protect both the add-in principal and the user policy.

**Accounting**

Accounting, also known as Auditing, provides rules for the use of emails. An email policy that is put in place can keep a companies’ network protected from numerous breaches such as security, legal liability, reputation damage, and confidentiality. It is unclear if Yahoo had these policies in place for their employee’s email accounts. However, if Yahoo had email policies in place, they would need to have a clear and set ser of rules and expectations based on specific criteria. By doing so Yahoo could have prevented this breach by detecting and blocking the phishing email that was sent out to employees thus preventing the massive data breach in 2014.

**Defense in Depth**

With little security provided by Yahoo and this data breach affecting so many people, it shows how important defense in depth is. Having multiple layers of security and detection can prevent attacks like these. Authentication, authorization, and Accounting are the concepts of triple A and play a very significant and crucial role in any security policy. Multi-factor authentication as mentioned above is one of the major security policies that should have been in place before these attacks happened. It would have prevented the hackers from accessing user accounts by flagging them as unauthorized users. Biometric authentication, although user preference based, could have protected many users affected by the data breach. Accounting logs what the user does and when they do it. By doing this it creates a trail allowing bad actors to be tracked allowing for detection of malicious activity.

**References**

Public Affairs, O. of. (2017, March 15). *U.S. charges Russian FSB officers and their criminal conspirators for hacking Yahoo and millions of email accounts*. The United States Department of Justice. Retrieved November 30, 2022, from https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

Fiegerman, S. (2016, September 23). *Did yahoo do enough to prevent the massive hack?* CNNMoney. Retrieved November 30, 2022, from https://money.cnn.com/2016/09/23/technology/yahoo-hack-timeline/index.html