Larry Arndt

CS-405

February 5, 2023

Case Study: Yahoo Data Breach 2013

In 2016 Yahoo announced that they had a breach in their records and that users should change their passwords. They did this as they were being acquired by Verizon and the estimated amount of accounts affected was more than a billion. With in a year Yahoo revised this number to up to three billion. In spite of this breach Verizon still purchased the company and yahoo proclaimed its commitment to security of its users.

So, what happened? This was a targeted “spear phishing” (Weinreb, 2019) attack made to trick certain employees into opening dangerous emails that contained virus programs. They did not know exactly how many Yahoo employees were targeted by the attacks by the Russian agents or how many of the emails were sent, but someone clicked on one, and it gave the attackers access to the user database and the Account Management Tool, used to edit the database. With the access they gained the hackers installed a backdoor so they could continue to remote in.

The tool did not let them do everything so they had to piece accounts together, but they got access to many accounts, and with that access could look at what ever they wanted. They targeted this company, because it had a large userbase of email subscribers, with sensitive data to exploit. I personally have used yahoo for more years than I can remember, at least twenty.

Potential and immediate threats were huge. One thing was that they did not notify people for years, and they probably knew before they did the notification. It seems they wanted the deal with Verizon to complete, perhaps and minimized how bad it was. That it went undetected was horrible and gave the hackers time to piece together the way to recover their way into accounts. (Williams, 2017) That is why it got so bad, and it did go on unresolved, it is hard to imagine if it would have gone on even longer, but it could have led to terrorist activities with identity theft.

Training your employees not to open links in their emails is the way to prevent this from happening. They should have a confirmation, like a two step-verification before opening links in messages. For me today, I call people on the phone if I get a link and ask them if they sent me something. To prevent future attacks yahoo should do the following:

With authentication requiring password changes every four months to six months and checking that the same password is not used up to two passwords back seems reasonable. Also, requiring strong passwords: length of at least 10 characters, an uppercase and lowercase letter, a symbol, and a number.

Authorization should keep personnel in the workplace on task, free access to the outside internet should be limited to a few terminals, and not connected to the whole of the network, you should run on a intra-net behind firewalls. Links trying to open anything external should be disabled, virus scans should be run on all files before they are opened.

Be more accountable, by logging and auditing who is accessing what accounts. They should have caught this breach quickly and put a stop to it. If an account shows a malicious access, it should be detected and reported tight away. They also need to inform the public so they can react. Building a system where an email program cannot gain database access is key.

Reference

Weinreb, Dan. “How Did the Yahoo Data Breach Happen?” *Dan Wein Reb*, 24 June 2019, [www.danweinreb.org/breaching-billions-a-look-into-the-yahoo-data-breach/#:~:text=In%202013%2C%20web%20service%20provider%20Yahoo%20broke%20the](http://www.danweinreb.org/breaching-billions-a-look-into-the-yahoo-data-breach/#:~:text=In%202013%2C%20web%20service%20provider%20Yahoo%20broke%20the).

Williams, M. (2017, October 4). *Inside the Russian hack of Yahoo: How they did it*. CSO Online. <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>