Yahoo, A Breaching Problem

An analysis by Kristof Marsolais

The Breach!

- Yahoo reported that 500 million user accounts were breached by a "state-sponsored actor"
- The problem was reported in 2016 (Fiegerman, 2016).
- The issue may have occurred since 2014 (Fiegerman, 2016).
- The initial user account total was 200 million user accounts (Swisher, 2016).

How the breach occurred

- The attack was most likely done with spear-phishing attacks which basically pretends to be an authentic link.
- The link then proceeds to download software that makes the compromised computer vulnerable to hacks.
- The hackers were successful in finding a computer and accessing the User Data Base (UDB) and Yahoo Account Management Tool (AMT) and copied them for their purposes (Battat, 2017).
- As a result of gaining access to the resources in the data base, they were able to use the given information to bypass admin access, unencrypted user data, logs, and passwords (Battat, 2017)

Results of the Breach

- Verizon was scheduled to purchase Yahoo's assets of $4.83 billion in late July (Fiegerman, 2016) days before the hack was reported.
- The news of the breach nearly threatened the deal that Verizon and Yahoo made since the report became public.
- The deal was still made regardless of the controversy attached, and Marissa Mayer left the company with $23 million (Kharpal, 2018).

Measures that Yahoo suggested to users

- An article on CNN gave a list of tips for users who had accounts hacked by the data breach (Kelly, 2016). They are listed here:
  - Change passwords often
  - Never use the same password twice
  - Pick better passwords
  - Update those security questions
  - Be alert
  - Turn on two-factor authentication

What should have been done

- Emails are a very crucial part in business today over 80% of business is conducted in public networks (Smallwood, 2014 p 190).
- What Yahoo needed to do was examine their systems and have multiple levels of access into their administrative tools.
- If the spear-phishing attack was a possibility, multiple admins should have checked the software update link before clicking it and confirming the possibility of a false update.

Conclusion

- When managing a significant database that holds millions of users, you should opt the user to use 2 step login procedures for their accounts for safety reasons.
- I deleted my Yahoo Email after this breach, created 2 step login for my current Email accounts, and have a retention policy of emails for 1 year.
- A recommended strategy by Randy Battat, who owns PreVeil, an Email security provider recommends that end to end encryption is used in these cloud databases. This basically severs any central points of attack protecting user accounts even when there is a breach (Battat, 2017).

References

- Battat, R. (2017, October 2). Risk management – lessons from the yahoo hack. Retrieved from http://www.rmmagazine.com/2017/10/02/lessons-from-the-yahoo-hack/
- Fiegerman, S. (2016, September 22). Yahoo says 500 million accounts stolen. Retrieved from https://money.cnn.com/2016/09/22/technology/yahoo-data-breach/
- Kelly, H. (2016, September 22). What to do if your Yahoo account was hacked. Retrieved from https://money.cnn.com/2016/09/22/technology/yahoo-hack-password-tips/index.html?iid=SF_LN