Yahoo Data Breach

Deziree Johnson

CYSE 300

Dr.Kovacic

Sep 10, 2023

The Yahoo data breach was a major cybersecurity incident that took place in 2013 but wasn't revealed until 2016, it is most notable breaches in history. In this paper, we'll take a closer look at what happened, looking at the weaknesses that were exploited, the individuals or groups behind the breach, the consequences Yahoo had to deal with, and what steps could have been taken to avoid or reduce the damage caused by this incident.

In the Yahoo data exposed several critical vulnerabilities within the company's cybersecurity infrastructure. These vulnerabilities include poor security practices, outdated software and Patching neglect, weak access controls, and poor monitoring and dectection. The Group that was credited to a hacking group believed to be connected to russian government. They used a combination of spear-phishing campaigns as well as malware to invade Yahoo. By infiltrating the accounts of Yahoo employees, the attackers initially got inside and then increased their access privileges to steal extensive amounts of user data.

Due to this significant incident, there were huge repercussions. One of these repercussions was user data exposure, about 3 billion Yahoo users personal information was exposed. The Exposure included email addresses, passwords, and security questions. This led to identity theft, and phishing attacks. There was also legal consequences, Yahoo countless lawsuits for delaying the information about the breach, which was a violation of the data protection laws. Not to mention the breach impacted Yahoos financials tremendously, which was shown when Verizon purchased it for $350 million dollars at a lowed price. As far as cybersecurity measures could have been taken to mitigate the consequences or prevent the incident, theres serval that could have be applied. For example, stronger encryption, employee training, access control, regular patching, Intrusion Detection Systems, and serval others.

In conclusion, the Yahoo data breach of 2013, though undisclosed until 2016, remains a big reminder of the need for strong cybersecurity practices. It showed the vulnerabilities in

Yahoo's security infrastructure, exposed by a group linked to the Russian government. The breach's repercussions included massive data exposure, identity theft, legal challenges, and financial impacts. To mitigate such incidents, organizations must prioritize cybersecurity, embracing stronger encryption, employee training, access controls, regular patching, and intrusion detection systems. This breach shows the importance of proactive cybersecurity measures in protecting user trust and a company's reputation in our increasingly digital world.

References

Schwartz, M. (2012). Yahoo Password Breach: 7 Lessons Learned. Informationweek - Online, Informationweek - Online, 2012.

Silverstein, E. (2016). The Cybersecurity Lessons In the Yahoo Breach. The National Law Journal & Legal Times, 39(4), 25.