Daoud Sogoba

CS-405: Secure Coding

Professor Hodde

November 16, 2021

The case is known to most as the Yahoo hack of 2013/-14. This took place in the early months of 2014 not too far off of Verizon’s aquisation of Yahoo. This case made the news due to the magnitited of compromsed assets as a result of the data breach.

The breach was initiated via a spear-phisinh email that was sent to an employee at Yahoo. More individuals may have been targeted, but the intrustion only required one to succumb to it. This link allowed the threat actor to gian acces to Yahoo’s user database and the tools by with the database was managed. This gave the individual full control over the database and the information that lied within. The individual was able to compromise the personal information too incude account information on over three billion users. Yahoo was targeted as over the course of its two decade history a large number of users have and continue to make use of its services. Some of the individals natuturaly are of high interest to Russian intellgicence agencies for reasions not important to the breach. The rammification of not resolving the issues around this breach will surley leed to more user data be compromised or more threat actors gaining acces to the data that is already compromised.

One of the most important wyas that this threated could have been prevented would be through the training of employees not click on links from non trusted sources. Perhaps a better system of layered security could have been implemented to prevent this from occurring. Granted, I'm not aware of these security in place or just how easy it was for the threat actors to access the database But, better forms of security like two factor authentication, multiple person authentication, or principles such as least amount of privilege could be implemented to prevent this in the future.