Win Inlaw

Professor Mimi Tam

Secure Coding

1 October 2024

**Case Study: Triple A & Defense in Depth**

The data breach we will be discussing is the National Public Data exposer of data. In December of 2023, two hundred and seventy million people were impacted by the disclosure of an estimated two point nine million records together. Sadly we have to say it made the news not right away. It only became public knowledge after in August 2024 the class action helped bring it to life. The data breach leaked social security numbers, names, mailing addresses, emails, and phone numbers of all two hundred and seventy million people. The company became a target of a group called USDoD which in April 2024 later on sold the stolen data for monetary gain. The immediate threat was in a plain archive until August 2024. A potential threat is everyone affected by the data breach must freeze their credit with all three major bureaus. Even suggestions for protection services. The developer could have prevented this hack by protecting administrator login information more securely. Having information like that in a more private function would allow it not to be as easily accessible. Having more password diversity could also help. Lastly, data management policy which of course included data classification. Helping protect data, particularly information that is highly sensitive is a vital part of any IT policy strategy usually. To summarize if employees do not share passwords and frequently update them could be a small contribution to avoiding hackers. Authentication needs to be tight. This will prevent unwanted use of the application. Even authorization needs to be so no one gets access to the network and steals sensitive data—secure devices only for secure authorization nly. Any company with password issues and other things of that nature must highlight the need for more cyber security to protect the company(accounting). Lastly applying Defense in Depth based on the mechanism of the initial breach remains unformed. Yet we can still determine the guess they need to maintain better updates on the system and better authentication when applying sensitivity and protectiveness.