Joseph Les

CS 405 Professor Hodde

Triple A and Defense in Depth

The Ticketmaster data breach, which occurred between April 2nd and May 18th, 2024, garnered significant attention due to the theft of over 30 million customers' sensitive bank information. The breach involved the exploitation of Snowflake accounts, accessed through a compromised third-party contractor, EPAM Systems. This incident underscores the vulnerability of organizations handling large volumes of sensitive data, making them prime targets for cyberattacks.

The immediate threat posed by the breach was unauthorized access to customer data, with the potential for ongoing exposure if the vulnerabilities were not addressed. Preventive measures, such as enforcing limited access controls, requiring two-person verification, and encrypting all stored data, could have mitigated the risk. The case highlights the importance of adhering to best practices, including robust authentication, authorization, and accounting (Triple A) mechanisms, alongside a defense-in-depth strategy. This multi-layered approach ensures that even if one security measure fails, others can still protect the system, thereby minimizing the impact of potential breaches.

References

Ticketmaster Data Security Incident. (n.d.). Ticketmaster Help. <https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident>

Zetter, K. (2024, June 17). Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake. WIRED. <https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/>