UNIVERSITY INSTITUTE of COMPUTING
Asia's Fastest Growing University

Experiment No. 7

Date: 26th April 23

Case Study: Security Issues in Zoom App

Zoom is a video conferencing application that gained widespread popularity during the COVID-19 pandemic due to its easy-to-use interface and reliable connectivity. However, as the number of users increased, security issues within the app were discovered, causing concern among users and potential risks to their personal information. This case study will explore the security issues faced by Zoom and how it impacted customers, as well as possible preventative measures.

How did it impact customers?

Zoom faced several security issues, including unauthorized access to meetings, video and audio interception, and data breaches. One major security concern was "Zoom-bombing," where unauthorized individuals would join Zoom meetings and disrupt them with inappropriate content. This created a significant impact on customers, who relied on Zoom for secure and private communication, particularly in sensitive meetings, such as those related to healthcare, finance, and government.

Another significant impact was the compromise of personal data. In July 2020, zoom paid $85 million to settle a class-action lawsuit that accused the company of sharing users' personal data with third-party apps, including Facebook, without obtaining consent. This data included email addresses, IP addresses, and device information. Such data breaches not only compromise customer privacy but also create legal and reputational risks for the company.

How could it be prevented?

Zoom has taken several steps to address the security issues faced by its users. These include enhancing encryption protocols, implementing multi-factor authentication, and improving privacy settings. Additionally, Zoom has introduced the concept of "waiting rooms" and unique meeting IDs to reduce the risk of unauthorized access to meetings.

One way to prevent such security issues is to conduct regular security audits and vulnerability testing. This can help identify weaknesses in the system and ensure that security measures are up to date. It is also essential to train users on best security practices, such as creating strong passwords, enabling two-factor authentication, and avoiding clicking on suspicious links.

Another approach is to adhere to industry standards, such as the ISO/IEC 27001 certification for information security management systems. Obtaining such certifications demonstrates a commitment to ensuring the security and privacy of customer data, thereby enhancing trust among users.

Conclusion

The security issues faced by Zoom highlight the importance of security and privacy in the digital age. While Zoom has taken steps to address these issues, it is crucial to remain vigilant and proactive in identifying potential vulnerabilities and implementing necessary safeguards. By doing so, companies can maintain the trust of their customers and ensure their privacy and security are protected.

********** **THE END** **********