King Saud University
College of Computer and Information Science
Software Engineering Department

SWE 477 Software Engineering Code of Ethics & Professional Practice
3rd Semester 2022/2023
Case Study

Facebook incident

Case study about the hacking of facebook servers in 2021

Name	ID
Reem alshareef	441200087
Shaden alayed	441201078

Section: 72141
Instructor L. Mashael Aldayel

Contents

1. Introduction :

WhatsApp, Instagram, and Facebook are frequently used applications that we
No table of contents entries found.
depend on and use daily, Facebook is a social media platform that allows users to connect with others and share content. WhatsApp is a messaging app that enables users to communicate with others, while Instagram is a photo-sharing app. but then we didn't ever imagine that it might go down or break for a long period of time until suddenly Facebook's main server which contains (WhatsApp, and Instagram) got hacked and the data of these platforms were stolen and everything suddenly stopped working for a long time, affecting millions of users. in the meantime, we didn't face something like this before and we didn't prepare ourselves for something similar, so our business and our needs were down. Meta platforms Inc (meta), formerly Facebook is a provider of social network advertising and business insight solutions. The metaverse focuses on developing a virtual environment that gives people the ability to interact and connect with technologies through its major product (Facebook, Instagram, and WhatsApp).
The company has a business presence across the Americas, Europe, the Middle East, Africa, and Asia-Pacific. Meta is headquartered in Menlo Park, California, the US.

2. Analysis of the Ethical Issue:

- Issue category:

The hacking of WhatsApp, Instagram, and Facebook in 2021 falls under the category of security ethical issues because it involved unauthorized access and theft of users' personal information, like email addresses, phone numbers, and location which can be used for unethical purposes such as theft of identity, which also exposed vulnerabilities in the software and systems used by WhatsApp , Instagram , and Facebook which can have serious implications for the security and privacy of their users.

- Consequences:

The hacking of Facebook, WhatsApp, and Instagram in 2021 resulted in a number of significant consequences. One of the immediate consequences was the loss of trust in these social media platforms. Users who had previously trusted them with their personal information, including their private messages, photos, and videos, were left feeling vulnerable and exposed. This led to a wave of account deactivations and a general sense of unease among users.
The hacking also had financial consequences for the affected companies. They were forced to spend significant amounts of money on cybersecurity measures and damage control. This included investigating the breach, repairing the damage, and compensating affected users for any losses suffered as a result of the hack.
The hacking also had social and political consequences. The unauthorized access to personal data raised concerns about privacy and the potential for misuse of personal information. It also highlighted the role that social media platforms play in shaping public opinion and the potential for these platforms to be used for malicious purposes, such as spreading disinformation or influencing elections.

- Reasons : Why did that happen?

The precise cause of the 2021 hacks of Facebook, Instagram, and WhatsApp is still unknown Yet it's assumed that a weakness in systems and software of Facebook enabled hackers to access users' personal data without permission, which led to the attack.

- Avoidance: what could have they done to avoid it in the first place?

The following steps may have been taken to prevent the hacking of Facebook, Instagram, and WhatsApp in 2021:

Frequent Security Audits: The companies should have implemented regular security audits to identify flaws in their software and systems at an early stage to fixed it before happening of attack.

Stronger Security Protocols: To secure user data the companies should have strong protocol such as two-factor authentication and encryption, or other stronger security measures.

Employee Training: Companies should have periodically trained staff members on how to detect and avoid security dangers .

regular updates : The companies should have made sure that all software and systems were up to date with the most recent security fixes.

- Mitigation techniques:

In order to mitigate the effects of the 2021 hacking incident, Facebook, the parent company of WhatsApp and Instagram implemented a variety of actions, Some of these actions were:

1. Resetting Access Tokens: In order to stop the hackers from accessing the accounts of about 90 million users, Facebook reset their access tokens.

2. Users who were affected by the security incident were informed by Facebook and given guidance on how to protect their accounts.

3. Coordinated Response: In order to look into the security breach and find the attackers, Facebook collaborated with law enforcement and other organizations.

3. Analysis of the Codes of Ethics

The professional codes of conduct, specifically the ACM/IEEE code of ethics, are relevant to the hacking of Facebook, Instagram, and WhatsApp in 2021. Computing professionals should follow the ethical principles and standards set out in the ACM/IEEE code of ethics to protect the privacy and security of users.

The following ACM/IEEE code of ethics principles are particularly applicable to the hacking incident:

Client and Employer

2.05 Respect confidality, Computing experts should protect users' personal information and respect their right to privacy. The hacking breach exposed the personal data of millions of individuals, jeopardizing their privacy.

Profession
6.02 obey all applicable laws unless, under special circumstances, doing so would be against the public interest

Self
8.02 computing experts should keep high standards of competency and continually work to expand their knowledge and abilities. This entails keeping up with the most recent security dangers and putting in place the necessary security measures to stop them.

The ACM/IEEE code of ethics offers direction to computer professionals on how to handle moral dilemmas and make choices that put user security and safety first.

- Which principles and clauses were violated?

The we totally agree upon that the principle of confidentiality was violated as users' personal information was stolen. Additionally, the principle of avoiding harm was also violated as users' personal information can be used for identity theft and other nefarious purposes. Additionally, the clause on respecting the privacy of others was violated by the hackers.

4. Law, Regulation, company policy

- How is it related to the law, Regulation, company policy?

The issue relates to the EU's General Data Protection Regulation (GDPR), which obliges businesses to secure users' private information and notify them of any data breaches. Additionally, the incident went against Facebook's own data security and protection policies, which call on the company to have strong security measures in place to secure user data.

5. Standards

How is it related to the standard of best practice? Which ISO standard do you suggest to avoid such issue?

- Related standard:

The issue is related to the ISO/IEC 27001 standard, which provides a framework for information security management systems. Implementing this standard could have helped Facebook, WhatsApp, and Instagram prevent the issue by ensuring that their systems were properly protected and that vulnerabilities were identified and addressed in a timely manner.[2]

- Suggested standard :

The ISO/IEC 27001 standard is a globally recognized information security management system (ISMS) that provides a framework for organizations to manage and protect their information assets. Implementing this standard can help prevent the hacking of Facebook, Instagram, and WhatsApp by ensuring that the organization has strong security protocols in place to protect user data and identify and address security vulnerabilities.
The ISO/IEC 27001 standard covers a range of areas, including risk assessment, security controls, and incident management. By implementing this standard, organizations can create a robust information security management system that is tailored to their specific needs and requirements.[2]

6. Conclusion:

- why did you select that ethical issue? what do think about that issue?

We talked about this ethical issue because it happened during a close period of time that we can all relate to, remember its consequences, and had been affected by it. Furthermore, we want to emphasize that nothing is 100% protected even if we use it for a long period of time and rely on it, and that every app needs a backup strategy if it becomes hacked or damaged. therefore, the hacking of Facebook, WhatsApp, and Instagram highlights the importance of strict security protocols and regular security assessments to protect users' private data. In order to prevent data breaches and protect customers' personal information, it also underlines the necessity for companies to follow standards like ISO/IEC 27001 and follow by legal frameworks like the GDPR.

7.References:

[1]"Meta Sues Hackers Behind Facebook, WhatsApp and Instagram Phishing Attacks," *amp.thehackernews.com*. https://amp.thehackernews.com/thn/2021/12/meta-sues-hackers-behind-facebook.html (accessed Mar. 24, 2023).
[2] International Organization for Standardization, "Popular standards," *ISO*, 2019. https://www.iso.org/popular-standards.html .
[3]Facebook, Inc. (2021). An Update on Facebook Security. Retrieved from https://about.fb.com/news/2021/04/an-update-on-facebook-security/
[4] Hackett, R. (2021). Facebook, Instagram, and WhatsApp Are Down. Here's What We Know. Fortune. Retrieved from https://fortune.com/2021/10/04/facebook-instagram-whatsapp-down/
[5] IEEE Code of Ethics. Retrieved from https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_ethics.pdf
[6]WhatsApp Security. Retrieved from https://www.whatsapp.com/security/
[7]Instagram Help Center. Retrieved from https://help.instagram.com/
[8]National Institute of Standards and Technology (NIST) Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework
[9] ACM Code of Ethics and Professional Conduct. Retrieved from https://www.acm.org/code-of-ethics
[10] Social Engineering Attacks on Facebook – A Case study Retrieved from https://www.researchgate.net/publication/356908456_Social_Engineering_Attacks_on_Facebook_-_A_Case_Study.