LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS5052NI Professional Issues, Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2021 -22 Spring Semester

Student Name: Aadarsha Muni Shakya

London Met ID: 20049438

College ID: NP01NT4S210023

Assignment Due Date: 12th May 2022

Assignment Submission Date: 12th May 2022

Word Count (Where Required): 3017

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

1. Introduction

While browsing the internet, search engines are important to look for what the users want. Examples or some top search engines are Google, Bing, and Baidu. Unlike these top-rated search engines, Elasticsearch is also a search engine but has a lot of vulnerabilities. Because of those vulnerabilities Social, Legal, Ethical and Professional issues are violated.

Elasticsearch is a portable, high-grade search engine that companies install to improve their web apps' data indexing and search capabilities. Many organizations use this for its benefits unaware about its flaws like server exposed without password protection. This violated the privacy of the users who used this search engine.

Not once, but the multiple times the security related flaws can be seen in Elasticsearch. Even though the search engine has vulnerabilities the owners or managers of Elasticsearch haven't taken any actions to fix the flaws. This will surely put the user's personal information exposed and therefore the security is not maintained.

Aim

The aim of this report is to analyses different issues of the given case study.

Objectives

- Learn about the given case
- Figure out its Legal Issues
- Figure out its Social Issues
- Figure out its Ethical Issues
- Figure out its Professional Issues

2. Background

In the given Scenario, multiple reporters like, Justin Paine, ZDnet, Bob Diachenko, and many more have found flaws and vulnerabilities in Elasticsearch's server. Some of those flaws and vulnerabilities are exposed servers without password protection, other security issues and database breaches. Despite having the knowledge of fixing those flaws, the business chose to leave the search engine vulnerable and compromise the personal information of people using their search engine.

Case study

Moreover, in this scenario ZDnet reported that online casino leaked information on more than 108 million bets which includes the customers' personal info, deposit, and withdrawals. This happened because Elastic search server was left exposed with no password protection.

Despite Elasticsearch being a high-grade search engine that helps with wed application data indexing and search capabilities, the security is very weak which led to the personal information of customers being compromised. Password is a basic thing which makes enhances security. So, without this a group of online casinos leaked information present in Elasticsearch.

Justin Paine, the security researcher found out the user data included a lot of sensitive information such as real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of played games. Which violated the privacy of people which can lead to problems like, spam calls and emails, robbery, cyber threats and many more.

Also, ZDnet is unclear how long the server was left exposed. This reflects that the managers and workers at Elasticsearch are very careless. The exposed server can lead to cyber-attacks like planting backdoor applications which will lead to information theft even if the server is protected with password.

Moreover, everyone has the right to maintain their privacy, however because of the leaky search engine the privacy is violated. And Elasticsearch is unclear about how many users were impacted, if anyone accessed the leaky server and if costumers were notified about this case so, the privacy was violated.

Elasticsearch is known for its multiple database breaches which makes it unreliable. For instance, a UK based security firm exposed Data Breach Database which stored huge information related security incidents from 2012 to 2019 with no password protection. So, trusting this search engine is like accepting to the personal data being breached.

Security researcher Bob Diachenko discovered the leaky database which data was very well structured. Despite having security problems, the management of data in Elasticsearch is very well structured. This can be good as well as bad. Good in a sense the data will be accessed is a quick and effective way. However, this will also make the unauthorized users learn and understand the information because it is very well structured.

Moreover, the leaked data included hash type, when the data was leaked, password, email, email domain and source of the leak. The database has the data included previously reported and non-reported security incidents which makes it more well-structured.

Also, Bob conformed that the information stored in the database related to prominent security included on adobe, Last.fm, Twitter, LinkedIn, Tumblr, VK, and others were true which makes Elasticsearch reliable at trusting information provided to its users, but unreliable because of its weak effort related to security so, the server was taken down within an hour after security alert.

The most recent server breach of Elasticsearch happened when protected personal information of millions of people and organizations were open. The data base was left open which led to the exposed data included detailed device data, links to photos and videos, and around 800,000 email addresses. This also violated the privacy of the people. The data included more private things like photos and videos.

Moreover, the Confidentiality is mainly compromised when the unauthorized users access personal information like data, photos, and videos. Whoever accessed the open data base will be considered as an unauthorized user even if they have no intentions on harming the information owner. When confidentiality is compromised CIA is compromised, which leads to lack of security.

In order to solve the security flaws in Elasticsearch search engine, experts point out breach occurs due to lack of built-in protections when there are no password protections or

firewalls. Moreover, Elasticsearch provided some recommendations on how to secure their servers, which include security authenticated sign-in, proper encryption, layered security, and audit logging.

Despite having the knowledge of those security concepts Elasticsearch chose not to use any of those services which makes this search engine un-trustable. This is because they don't have much value towards their costumer's privacy and security. In an organization stakeholders like customers should be valued the most. This is because they use goods and services in exchange of money. And if Elasticsearch doesn't act to improve its security they will go out of the search engine service providing business.

3. Legal Issues

Legal issues include the laws, rules, and regulations an organization was unsuccessful to provide. Moreover, all laws which include policies, methods, means, and standards required to maintain confidentiality, integrity, and availability to its customers. If those three components are fulfilled the user's data and information is secured.

In this case, an online casino group leaked information of more than 108 million bets. The information includes details about customers' personal information, deposits, and withdrawals. This incident compromised the security of confidential information of its customers. This happened because a search engine called Elasticsearch left its server exposed without any password protection. This directly arises a legal issue where the method used to protect its server by a password is not configured which led to the leaked information. Furthermore, the leaked information compromised the security of people involved in those leaked information.

Similarly, ZDnet reported that they are unaware about unclear how long the server was left exposed online, how many users were impacted, if anyone else accessed the leaky server , and if customers were notified that their personal data was left exposed. The policies should cover the overall activities of an organization. However, Elasticsearch is unaware about its own server and taking this case as an example, they don't have proper policies in their organizations to maintain legal issues. This is the main reason the managers at Elasticsearch were unaware about its resources and configurations.

The cases mentioned above are small data breaches, an incident where five billion records were exposed after an UK based security firm exposed its data breach database was reported. The standards of a search engine should be secure and trustworthy. The basic standards of an organization are password protection but in Elasticsearch there is no password protection which leads to confidentiality of information being compromised. This way Elastic search has violated legal issues multiple times.

Bob Diachenko also discovered this leaky database and noticed the data was very well structured. This proves that Elasticsearch is just concerned about policies related to improve their web apps' data indexing and search capabilities. Whereas the security should be their top priority because if Elasticsearch is secure the customers will trust the search engine and will

grow as leading search engines. However, they are not concerned about their security which led to multiple legal issues related to unauthorized access of information. After this incident was reported, the server of Elasticsearch was taken down to minimise the potential harm to the users in the future.

The most recent server breach occurred when an app developer left the Elasticsearch database open which led to more sensitive information such as detailed device data, links to photos and videos, and around 800,000 email addresses. In this case, app developer who works for other organization is changing the settings of Elasticsearch servers. This means not just virtually security, physically security is also a legal issue in this organization. There should be policies and security to allow authorized managers and workers to enter the room and restrict other unauthorized users like Peekaboo's app developer.

4. Social Issues

The issues that impact the society is known as social issues. If an organization decimates its employees based on their race, then the act is a social issue. In this scenario, a search engine called Elasticsearch has violated multiple social issues which is described in the paragraphs below.

At first, this search engine has a very bad reputation in the society, this is because the employees in this firm are very careless. An app developer can walk into their server room and modify changes like leaving the database exposed is a very careless behaviour. And such careless behaviours will lead to the bad impression on the society. Furthermore, the information from the open database can be accessed by anyone on the internet which arises a social issue of bad reputation in the society. So, those careless behaviours should be minimised.

Similarly, another social issue which will ruin the reputation of this organization is not wanting to secure the data of their users. In this case, security experts suggested the breach occurs due to lack of protections such as password and firewalls. Moreover, Elasticsearch also provided some mitigation strategies like secure authenticated sign-in, proper encryption, layered security, and audit logging. This will show that Elasticsearch doesn't care about security and privacy of sensitive information. Such acts can ruin the reputation of Elasticsearch in the society which means it is a social issue.

Society is a group of people who live in the same environment. In this case, the leaked data by Elasticsearch can be of anyone on the society. This leads to society members information being unsecure and exposed. This is a social issue because the privacy and security of information in the society is violated by Elasticsearch. For example, more than five billion records were exposed by Elasticsearch because it was stored without password protection these type of incidents will violate the privacy of people in the society and actions should be taken to fix them.

Moreover, those leaked information can be accessed by unauthorized users who can misuse that information. For illustration, if a spammer gets the leaked information like real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of

played games they can use this information to create a more effective spam message or emails. For example, a spammer can send fake updates based on the system knowledge gained from the leaked data and the victim might think the update is legit and therefore spamming will be successful.

More severe cybercrime like, blackmailing can happen because of the leaked data. In this case, links to photos and videos of users were exposed when the database was left open. Those leaked photos and videos can be private and if blackmailers get hold of those private photos and videos, they can use it to blackmail the actual owner of those photo and video which might lead to victims paying the ransom amount. This is social issue which might occur because of Elasticsearch.

5. Ethical Issues

When an act, decision, or scenario creates conflict with the society's moral principle ethical issues occurs. Depending on the society the ethics can be different. For illustration in Hindu culture when a person dies wearing white clothes is suggested. Whereas for Christians white is wore in weddings. So, both examples are ethical in its own society and might create conflict in other society.

In this case, the concept of not using password protection or leaving the database server open are bad moral principles. This is because the act of Elasticsearch is directly compromising the security and privacy of their users. This is an unethical act which can be considered as an ethical issue. If managers or owners of Elasticsearch had good moral principles, they would consider the privacy of their users which therefore would have been ethical. Therefore, not using password protection has shown bad moral principle of Elasticsearch which is an ethical issue.

Moreover, an unethical act like irresponsible actions which hampers the security is an ethical issue. In this case, the irresponsible act will be allowing Peekaboo's app developer to access the server room and make changes to it. Changes like leaving the Elasticsearch's database open which led to 70 million log files which was stored March 2019 exposed on the internet. The leaked data includes stored detailed device data, links to photos and videos, and around 800,000 email addresses. So, this act done by Elasticsearch is very irresponsible and therefore violated the ethical issue.

Other ethical issue includes compromised confidential information is done by Elasticsearch. Those confidential information includes, customers' personal information, deposits, and withdrawals, real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of played games, hash type, leak date, password, email, email domain and source of the leak, and lastly detailed device data, links to photos and videos, and around 800,000 email addresses. Not just ones but in multiple occasions that confidential information was left exposed which compromises the confidentiality of the customer's information.

The decisions made by not making the security of Elasticsearch secure is an ethical issue. This decision by Elasticsearch can be to save cost. They want to save money by not implementing security concepts like password and firewalls. This decision of compromising the customer's information by not using any safeguard is an unethical behaviour. By this action the right of privacy of information of the customers is also violated. Therefore, not using safeguards like passwords and firewalls to protect sensitive information and save cost is an ethical issue.

Everyone has the right to know about their personal information. However, in this scenario, the researchers are unaware about customers of Elasticsearch were notified that their personal data was left exposed. Those personal data included sensitive information, such as real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of played games. This violated the right to know about personal information which is an ethical issue.

6. Professional Issues

Professional issues dealt about ethical or practical activities that determine good or bad professional practice in an organization. The mixture of good policies, effective resources, and responsible authority will make an organization's professional issues minimum. However, in this case Elasticsearch lack in policy making, resources and authority.

For policies, they can limit a person or stakeholders' action in an organization. From restricting workers to access infrastructure to not using social media can come under policies. And if those policies are violated legal action can be taken. In this case, Elasticsearch has lacked in making effective policies. A simple policy of not allowing unauthorized people to access database would have saved 70 million log files. Peekaboo's app developer is an unauthorized individual and this policy will make him liable for all damage because it was his fault and detailed device data, links to photos and videos, and around 800,000 email addresses were leaked.

In Elasticsearch the authorized people like managers are misusing their authority, even though they are aware about password protection they chose to leave the server and database without a password. This led to the dada being breached and accessed by unauthorized users on the internet. Misusing authority can be considered as a professional issue because this act is unethical in a professional point of view.

Also, the important it resources like firewall are not implemented by Elasticsearch. This is Elasticsearch giving less priority to security and compromising the privacy of the users. This can be seen as discrimination towards security related gadgets since they know about those gadgets yet chose not to implement it. This is a professional issue of Elasticsearch because it is unprofessional to keep other person's data exposed without any consent.

Elasticsearch search engine has no password protection, firewalls, secure authenticated sign-in, proper encryption, layered security, and audit logging. This makes it untrustworthy and the concept of improve web apps' data indexing and search capabilities will not be met. This will create unrealistic and conflicting goals within that organization.

Therefore, this will also create professional issues because the organization will not run as planned.

7. Conclusion

For conclusion, Elasticsearch is a vulnerable search engine which doesn't have any password protection or other safeguards which arises several issues like Legal issues, social issues, Ethical issues, and Professional issues. This scenario of Elasticsearch affected the people or organizations who used the service of Elasticsearch. The data and information of those customers were compromised.

In this case, the authority of Elasticsearch is very poor. From policies to physical security, nothing was managed which led to those issues. If the managers or authorized people are changed the act of not configuring password protection, firewalls, secure authenticated sign-in, proper encryption, layered security, and audit logging will be changed, and those safeguards will be configured and therefore those issues will be solved.

8. References

cimpanu, C., 2019. *Online casino group leaks information on 108 million bets, including user details | ZDNet.* [Online] Available at: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/
[Accessed 12 May 2022].

Law Insider, 2022. *Security Laws Definition | Law Insider.* [Online] Available at: https://www.lawinsider.com/dictionary/security-laws
[Accessed 12 May 2022].

My Accounting Course, 2021. *What are Ethical Issues? - Definition | Meaning | Example.* [Online] Available at: https://www.myaccountingcourse.com/accounting-dictionary/ethical-issues#:~:text=What%20Does%20Ethical%20Issues%20Mean,question%20from%20an%20ethical%20standpoint.
[Accessed 12 May 2022].

Newberry, C., 2020. *Social Media Security Tips and Tools to Mitigate Risks.* [Online] Available at: https://blog.hootsuite.com/social-media-security-for-business/
[Accessed 12 May 2022].

Sweeney, M., 2022. *Ethical dilemmas in computer science | ZDNet.* [Online] Available at: https://www.zdnet.com/education/computers-tech/ethical-dilemmas-computer-science/
[Accessed 12 May 2022].