Cyber Security Threats And Vulnerabilities And Risk

1. Abstract

The world is changing, as is its necessities and development. Apart from all the basic factors, technology has been a fundamental cause for development almost all around the world. With technology and computers evolving at this speed, it is obvious to encounter its threats and vulnerabilities. For all the positive reasons, cyber security has been a prime cause for mitigating a large amount of threats and risks in the cyber world. The companies and its users have been needing to invest millions to billions on recovering from these kinds of incidents which is certainly not a factor to be overlooked. Henceforth, this report will be discussing a similar incident that occurred with Uber which was not long ago in late 2016. The case was about illegal access to the user data of Uber that was stored on a third-party cloud-based service without appropriate consent. However, the incident was only limited to the data and not any infrastructure or corporate systems. The two individuals who hacked the data had information about the names and their respective driver's license numbers of approx. 600,000 drivers along with some personal information on 57 million of uber users throughout the globe. This information included phone numbers, email address, names. Due to the uninvited incident, Uber had to take a huge step to shut down the further unauthorized access to everyone. Hence, Uber was a mess! However, the culprits had been identified and was assured that the lot of data that were leaked were destroyed immediately. [1]The primary cause of this attack is observed to be the poor management of identity access of the company itself. It could be entitled as AWS identity and access management theft.

2. Introduction

Access management and AWS identity is known to be a web-based service that helps the users to securely control access to the resources. Companies and organizations need IAM in their security planning, as it is crucial to control who is authorized and authenticated to use the resources. About its functioning, when we create an AWS account, we begin with a single sign-in identity that has a full-on access to entire AWS resources and services in the account. The so registered account is called AWS account root user and will be accessed by simply logging on with the email address and password with the same email address that we used in order to create an account.

Here are the few features that IAM has to offer for the companies that they are holding up.

Shared access to your AWS account

We can gain permission to administer and use resources in our respective AWS account without needing to share access key and passwords.

Granular permissions

We also can grant different permissions to different individuals for different resources i.e. it just

works as an Email, as we can relate, we can send mail different topics to only selected individuals at around the same time while giving allocated information to users with respective priority. [2]

(MFA)Multi-factor authentication

It is possible to add two-factor authentication to the account and to the individual end-users in order to strengthen the security. With MFA it’s not only an access key or password that we have to provide but it also requires a code from a device that is configured specially.

Identity Theft

Above was a brief introduction about Identity Access management and how the company uses it. However, coming back to our report, we are to discuss in the topic of identity theft bringing the scenario of Uber in the limelight. Identity theft is when a certain hacker has gained access to our personal and private information (name, address of residence, email address, bank details) which are normally for the evil purpose of acquiring benefits or stealing money from the company. A small detail can actually be used to find out a lot more of details about you, such as a single photograph, our birthdate and even information’s about your own family.

If a hacker tries to steal your identity and gets successful, they may have a lot of possibilities with them such as.

- Open a legitimate account in your name which can possibly build debt that can solely ruin your credit history.
- Open a phone line or even the internet in your name.
- Extract the benefits from the government in your name.
- Commit a false use of your name to commit criminal activity.
- Misrepresent your identity via social media.
- Use your name as false tax refunds.

People are often mistaken is the assumption that identity theft only occurs to wealthy people whereas, it is a sad reality that anyone could be fallen as a victim regardless of their wealth. However, in terms of our topic, it could be addressed as Financial Identity Theft. Financial identity theft has variable meaning in nature i.e. Either the victim’s identity is used in credit cards or bank accounts in order to use illegally by withdrawing money or limit out the credit cards or, the hackers could make false use of the identity by issuing loans and so on. In our case, the hackers had sneaked a huge amount of personal information’s and were asked for a ransom of $100,000

Which they, unfortunately, had to clear up to delete the stolen personal information hence keeping the breach shut down as per the reports and articles on them. [3]Programmers have effectively penetrated various organizations as of late. The Uber rupture, while substantial, is overshadowed by those at Yahoo, MySpace, Target, Anthem and Equifax. What's all the more disturbing are the outrageous measures Uber took to shroud the assault.

3. Literature review

The troubles have been sorted already looking at the current time frame. Uber has still proved to be on the top regardless of everything. It is a practical app. Prior to the routine, lifestyle, and somehow something that almost majority of the public users depend on. However here is how its reported as how this all really occurred. Kalanick, former CEO and co-founder of Uber only got to know about the hack in late 2016 which is on November, after a month after the incident took place. The company has to say that Uber has just cleared the lawsuit with the attorney general over data security disclosures on New York. He declined to post any comments on this matter. To be clear about how the hack went down, two attackers used login credentials by accessing a private GitHub coding site that are used by uber software engineers where the hackers found archive of information about driver and rider. Eventually, they had an uber email about the ransom money.

With regards to Law and political views, Uber has lit charged political exchanges globally. A couple of governments are concerned over the control the sharing economy. From one point of view, while the sharing economy and Uber have their masters, they similarly have their cons. Uber's rising has problematically influenced the matter of other traditional taxi organizations. This has offered a climb to the opposition which even turned political at a couple of stages. Without a doubt, even the specialists are worried in case they need to bring new laws for the associations like Uber. There is no uncertainty about Uber's predominance among its customers. Uber has a customer-driven business approach that prompts a low-edge advantage for drivers, and they don't slant toward in any way shape or form. Uber does not need to take after standards as standard drivers but instead, they are as often as possible fined for avoiding the bearings. France, Germany, India, the United Kingdom, and the Netherlands are a couple of countries that have fined Uber. Thusly, Uber needs to tackle its weaknesses and experience openings by using its quality and overcoming risks against the association. [4]

Uber has its own charges that were to be dealt with. There was a possibility of Uber facing consequences from both federal and state agencies. The agencies had given 180 days to give an audit report into security and privacy practices. Uber had gained international attention as it is an incident of multiple countries such as the USA, the U.K., Australia, Italy, Philippines.

4. Main Body

4.1 Know the Enemy

Uber is the biggest ride service provider in the world and new companies like DiDi and Ola trying to capture that thunder, they would be glad to gain private information on Uber. Any black hat hackers trying to sell information to their competitors in the market. Hackers will try to get access of their information in order to blackmail or threaten the company. This can get Uber to expend a lot of money to keep the hackers from leaking their or their customer's private information or face the backlash and loss of reputation on the market. And the worst thing that Uber can face now is being deemed being not so reliable. This can truly plummet Uber’s reputation and market value to the ground. [5]

4.2 Know the self

When it comes to security reliance, Uber hasn’t been doing so well in recent days. With its recent scandal of leaked private information of its 56 million users, it is still trying to get back

from that hurdle. With its enormous market share in hand, it wouldn’t want any of these mishaps causing them another reputational havocs.[6] As it might just affect significantly on its business name and its values. So, when it comes to uber it must have realized its security shortcomings and improving it would be the foremost priority.

4.2.1 Vulnerabilities

Uber should be aware of its vulnerabilities in the field of cyber security. With its recent outbreak of backlash due to its inability to secure the private information of its million users, it is clear as a day what its vulnerabilities are. With better vulnerability and multiplied susceptibility to attack, mobility is highly unprotected in comparison with business enterprise network infrastructure and greater so than the one-third cloud-based structures related to Uber's records breach. This is largely thanks to unsecured mobile gadgets that offer a backdoor for cyber threats into in any other case relaxed infrastructure - dramatically increasing an enterprise’s vulnerability to assault. [7]

4.2.2 Threats

With such a bigger userbase comes real big threats. Threats include access to millions of personal information that could possibly lead to identity theft to access of their credit card information that could lead to a lot of damage of a lot of people’s revenue. With the rise in new markets and drivers, data theft, scam, and scandals are also on rising. This can harm the brand in a devastating way. And even looking at the future of Uber, Google cars might just replace Uber in the long run. So, it also poses a huge threat in its market share. This makes it even harder for Uber to make too many of these mistakes. Uber undoubtedly must have had tougher access control given its large userbase and equally large data. Kelly Sheridan “Attackers initially accessed a private GitHub coding site for Uber software engineers, where they found credentials for an Amazon Web Services account containing users' information.”

And the hardest part for them to swallow was that this wasn't a sophisticated attack. According to Imperva CTO Terry Ray, “Uber's decision to use live production data in an online platform where credentials were stored in GitHub was quite questionable.” This allows developers to frequently practice live production data in testing. This information is 'almost never monitored or secured' and every so often is stored in numerous locations. [8]

4.2.3 Risks

The implication of this is that businesses making use of cell technology to boom productivity are extensively extra vulnerable to cyber-threats. IBM discusses this of their 2017. Price of records Breach examines', suggesting that mobility no longer handiest will increase the complexity of IT safety and a corporation’s ability to reply to statistics breaches, however, it additionally prolongs facts recuperation, reaction time and raises the expenses associated with a statistics breach. these prices may be huge for organizations, with IBM approximating the fee in keeping with the breach at $7.35million. this does not account for a way an employer's recognition might be damaged, or the viable compliance ramifications for senior control related to failing to reveal a security occasion, a component obtrusive for Uber, who's going through multiple investigations via state governments after their failure to document the data breach. agencies should recognize that the excellent manner to avoid the outcomes of a cyber breach is to put together for and prevent cyber threats.

4.2.4 Cost of addressing the risk

The cost of addressing the risk of cyber security can be millions of dollars compared to the large userbase and the huge amount of data. But it is clearly a much smaller price to pay compared to what they paid in their recent outbreak. Uber recently revealed that the private information of around 57 million customers had been exposed due to a security breach. Uber also tried to hide the breach for over a year which adds to its criticism. [9]

4.2.5 Role of security Policy

Security guidelines are the inspiration of great protection software. With described protection regulations, people will recognize the who, what, and why regarding their agency's safety software, and organizational risk can be mitigated. [10]

4.2.6 Role of standard

Certainly, the first rate-regarded standard for the usual management of data safety is ISO 27000 – really a circle of relatives of standards (nicely over forty in total). ISO 27001:2013 particularly is a chance-primarily based popular method for the data protection control gadget. It adopts an international vision of the commercial enterprise, manner, human beings and technology dangers, and pinnacle control is actively involved within the complete threat mitigation manner.

4.3 Method used in CISCO SAFE Model

CISCO SAFE Model subtleties the security intends to ensure a framework against any sorts of digital dangers, vulnerabilities or dangers by appropriately preparing and giving out jobs-based structure streams that verify the necessities of the organization. In Business-based security, it has got VPN, Web security Applications, Wireless rogue detection, and WIPS with respect to Server-based security, it drills down Anti-Malware, Anti-virus, and Cloud Security. Numerous amount of companies uses this method as it is technically a better option. [11]

5. Conclusion

In conclusion, cyber security should have come up clean in the first place as the majority agrees on it. The company should have somehow had a stronger security measure for that lot amount of collection of data. [12]We also have concluded that covering up cyber-attack would be a bigger mistake than that of crime.

6. Future works

In future works, there could be a lot of improvements in the models and the guidelines in a way of cybersecurity. We should be able to identify the threats such as unauthorized access to computers must be prevented before any losses and leakages. Using of two-factor authentications in a company could be a good increment in the security measures. Conducting audits punctually and on a regular basis since, when a company starts to grow it is unacceptable to compromise in the terms of security of our data. And finally having an In-Depth knowledge about the affecting factors and planning accordingly would be a valuable point. Uber

however has been rising regardless of having its reputation at stake. And it has solely kept promises to be preventive about threats in the future.