International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 468-470
Published Online June 2020 in IJEAST (http://www.ijeast.com)

DATA BREACH- AN OBLIVIOUS THREAT AND ITS CONSEQUENCES

Soumya Jaiswal
BCA student
Department of computer science
Kalinga University, Atal Nagar, Chhattisgarh, India

Rahul Chawda
Assistant Professor
Department of computer science
Kalinga University, Atal Nagar, Chhattisgarh, India

Abstract: Data breach has become one of the serious problems in recent years as with the increase in technology the threat of data security is increasing. This paper mainly focuses on giving information about causes of data spill and prevention methods an organisation or individual should adopt to prevent themselves from such a threat.

Keywords- Data breach, Data security, Data spill, Smartphone data breach.

I. INTRODUCTION

Data breach which is also known as Data spill or data leak is an intentional or unintentional revelation of one's private or confidential information which can be his credit/debit card number, social media passwords, bank details, personally identifiable information etc. Data breach is something that every company should be aware of irrespective of its size as it results in the loss of millions of records and sensitive data, attacking not just the breached organization but also everyone whose personal information has been registered with the organization.

II. WHO CAUSES DATA BREACHES?

It's a general thought that data breach is generally caused by an outsider but can also be caused by following:

1. Malicious Insider: Person working in an organization shares the data with the intention of causing harm.
2. Lost or stolen device: An unencrypted or unsecured device if lost can be in risk of breach.
3. Malicious outside criminals: These are criminals who use vectors to gather information from an organisation or individuals.
4. Accidental Insider: It can be an employee or ex-employee who accidentally or unintentionally read the file without permission, as it is read by an unauthorized, data is considered as breached.

III. INTERNAL VS EXTERNAL DATA BREACH IN AN ENTERPRISE

It's a general thought that mostly data breach is caused by black hat hackers or any external medium but that's not true instead those working in companies and organizations are the major cause of data spill.

According to Clear Swift Adaptive cyber protection 58% percent of the data breach is caused by insiders and rest 42% by outsiders.

Internal breach is more likely to occur as employees have access to sensitive information on a regular basis, they may leak information at greater ease than that of an outsider. Furthermore data leak can also be accidental whether by attaching the wrong file to an email or by losing laptop or USB drives with confidential information in it.

Internal breach can be more deleterious as an attacker can copy a large number of files having information stored without any knowledge whereas external attackers attack an outward facing connection, which

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 468-470
Published Online June 2020 in IJEAST (http://www.ijeast.com)

has deeper security. Tools which are responsible for external hacking such as SQL injection are limited in resources hence cannot get access to complete information.

IV. HAS THE SECURITY OF YOUR MOBILE DATA BEEN COMPROMISED?

In the past few years smartphones have become a crucial part of our life. We not only use it for communicating with each other but also use it for online entertainment and business related purposes. But their popularity, portability and precarious security make them attractive targets for cyber criminals.

Mobile security has not always been on the top of mind, more unsecured smartphone application means more vulnerability. According to the Checkpoint 2019 Cyber Security report, 59% of people working in an organisation don't bother about threats hence don't use mobile threat defense solutions capable of detecting threats such as malware, Man-in-the-middle-attacks, mobile ransomware attacks etc.

V. THE ACTUAL FACT BEHIND BAN OF CHINESE APPS IN INDIA

As most of the people still think due to patriotic sentiments these apps were banned in India but the actual reason behind this is the threat of data breach. These apps secretly and illegally send vast amounts of personal data to China which raises serious concern about the country's security. Among 59 banned apps let's take example of the most famous app Tiktok how it is involved in breaching. According to IOS 14 this app is capable of snooping data copied on clipboard which is a serious privacy concern, when coming to the permission part the app doesn't even ask permission for location access and takes region data from your sim card and IP address. The app gathers a trove of data about its users, including their phone and social network contacts, email addresses, IP address, location and other information, according to the lawsuit.

VI. OVERVIEW OF SOME COMMON SMARTPHONE SECURITY THREATS

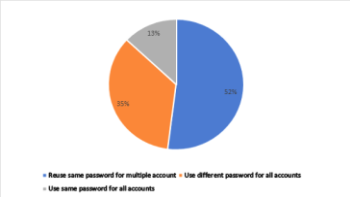
- **Social engineering/ Phishing:** Phishing or social engineering are the major cause of smartphone breach. According to a 2018 report by security firm FireEye 91% of crime starts with email. They rely on tactics to make users click on dangerous links by showing some special offers or something impressive hence people provide them with their sensitive information. Mobile users get targeted easily because many clients display only their name in email notification so attackers imitate to be someone trusted you know hence take advantage. It's not just email anymore, instead over the past two years 86% of the attacks took place outside the inbox such as google or WhatsApp along with many games available online. It can be prevented by various methods such as using anti-phishing software, by watching out for shortened URLs, checking on punctuation and grammar of URLs, using sites that have SSL certificates etc.

- **Man-in-middle attack:** In MITM attack a cyber actor intercepts the communication between two parties, impersonates both parties and tries to access the information shared between both the parties. Public Wi-Fi networks such as those in cafeterias, railways and airports provide an opportunity for MITM attacks. It's not that hard to decrypt signals these days so if you are not using VPNs then it means you are leaving a door open to attackers. They mostly capture data transmitted as credentials, emails, data submitted to web forms and so on.

- **Rogue Apps:** Installing unsecured and rogue app again opens the door for cyber-attack. Unauthorized apps collect the browser history, location details, contacts lists etc. and sell it on a rogue server. They are capable of doing this as they contain malware such as Trojan and viruses which are capable of stealing information. As rogue apps are fraudulent versions of credible apps it's too hard to spot the difference between the two. So the most appropriate way to protect yourself from this threat is to use only trusted app stores for downloading applications instead of any websites or so. You can identify rogue apps by checking download sites, terms and conditions, ratings and
Permission.

- **Poor password hygiene:** As per the survey it is found that only 35% of the people use different passwords on different accounts and nearly a third of the population doesn't use 2FA which is equally worst. Only a quarter of people use password managers, which suggests a majority of people use weak passwords. It is found that in 2017 80% of business breaches were related to poor or stolen passwords.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 468-470
Published Online June 2020 in IJEAST (http://www.ijeast.com)



It is seen that employees often use the same password for both professional and personal uses. If we use the same password often the chance of getting breached increases as if one account gets hacked other can also be hacked.

VII. SIMPLE STEPS THAT CAN HELP YOU TO REDUCE SMARTPHONE DATA BREACH

1. Look over all the applications linked to your account and you have granted permission to access.
2. Use VPN if using public Wi-Fi.
3. Keep stronger passwords having alphanumeric characters with a mix of special characters and always turn on 2FA.
4. Minimize the use of third party apps and websites.
5. Optimize your lock screen security.
6. Always keep your mobile apps updated.
7. Beware of scams and phishing emails
8. Only charge your phone on trusted USB ports.
9. Always download apps from trusted app stores.
10. Use trusted anti-virus software.
11. Use websites such as *haveibeenpwned.com* to check whether your email is compromised for breach.

VIII. CONCLUSION

Data breach is leak of confidential and private data so, preventing and detecting data breach is an indispensable process. In this paper I have presented some ways in which an organization and individual can prevent themselves from such serious security threats and how to protect their smartphone from various vulnerable threat.

IX. REFERENCE

1. Raphael, J. (2020). 8 mobile security threats you should take seriously in 2020. https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html
2. Irwin, L. (2020). How do data breaches happen? Understanding your organization's biggest threats - IT Governance UK Blog. https://www.itgovernance.co.uk/blog/understanding-the-different-types-of-data-breaches
3. Top 7 Mobile Security Threats in 20 July 2020,https://www.kaspersky.co.in/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
4. Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211. doi: 10.1002/widm.1211
5. 8 Most Common Causes of Data Breach Sutcliffe Insurance. https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/#:~:text=Hacking%20attacks%20may%20well%20be,or%20lost%20(stolen)%20passwords
6. What is a data breach? https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html
7. Cybersecurity and Training. 2020. *External Vs. Internal Cybersecurity Risks: Know The Difference* https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference
8. It Still Works. 2020. *Difference Between Internal & External Threats To An IT Database*.https://itstillworks.com/difference-between-internal-external-threats-database-26979.html