IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Leakage: Threats And Prevention

Khan Mantasha Wasi Ahmed
Department of Information Technology, B. K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan, Maharashtra, India

Abstract: Due to COVID-19 ,whole world is connected digitally. Every single humanoid is accessible,doing their respective work from home. Process of passing authorized and unauthorized data is everyday work now. This led risk of data security and different threats. Now its a everyday news of hitting data breach. Leaked Data can be used for many purposes, and can cause damage for any individuals.

The data leakage can be unintentionally or intentionally for the third party. In this paper, I have explained what is data leakage and major problem of data security. Also ,threat by the guilty party and furthermore some prevention and future anticipation.
Keywords: Data leakage, Data Security, threat, Data Breach, prevention

I.Introduction

Today ,world is consistently passing the information from one person to another person. The first person or the distributor must assure that the sent data is safe and secure. Data can be sensitive for any individual, irrespective of their work and age. Data leakage can be done by any internal or external employees,rivals or any other person for different purposes. They can misuse web services, email services, cloud services, optical media, and laptops. Data security experts must come with a solid solutions to prevent these malicious practice of data leak.Data security must be implemented to avoid leakage.

In this paper , I have explained data leakage its type and what can be the purpose behind it. Also some must taking step to prevent data loses.

Data leakage

Data leakage is also known as low and slow data theft,now its a massive problem of data security, damage caused to any working livelihood or organization, regardless of size or industry, can be critical. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.

Types of Data leakage

1.Data Breach

A data breach is an incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner.A data breach might involves the loss or theft of Social Security number, bank account or credit card numbers, personal health information, passwords or email. A data breach can be intentional or accidental.

The Accidental Breach

Sometimes unauthorized data leakage does not mean intended or malevolent.for example,sometimes an employee may choose the wrong receiver while exchanging the confidential data. Unfortunately ,unintended data leakage cause the same damage and penalties.

2.The disgruntled or III-Intentional Employee

When we think of data leakages, we think that data held on stolen laptops, phone or data that is leaked due to email or other electronics. However, majority of data loss does not occur over an electronic medium; it occurs via printers, cameras, photocopiers, removable USB drives and even dumpster diving for discarded documents. an employee may have signed an employment contract that effectively signifies trust between employer and employee, if they are leaking confidential information out of the building if they are disgruntled or promised a hefty payout by cyber criminals. This type of data leakage is defined as data exfiltration.

3.Electronic communications with malicious intent

We widely use the electronic communication,any organizations give employees access to the internet, email, and instant messaging as part of their role. The fact is that all of these mediums are capable of file transfer or accessing external sources over the internet. Malware is frequently used to target these mediums and with a high success rate. For example, a cybercriminal can easily spoof a legitimate business email account and request sensitive information to be sent to them. The user would unconsciously send the information, which might contain financial data or sensitive pricing information.

II.Methodology

Latest Data Breaches

BigBasket data breach
In November 2020, the Bangalore-based online grocer BigBasket faces a data breach that leaked the details of their over 2 crore users, including email IDs, phone numbers, order details, and addresses.

Justdial Data Breach
In April 2019, the Mumbai-based local search engine Justdial went through a data breach that leaked details, including names, mobile numbers, email ids, occupations and addresses of nearly 10 crore users.

Air India Data Breach
On 21 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

Dominos India Data Breach
On 22 May 2021, it was reported that Dominos India, subsidiary of Jubilant FoodWorks, had witnessed a cyberattack and the data of 18 crore orders were leaked on the dark web including all the order details, email addresses, phone numbers and credit card details.

A quick skim of those breaches by mob sector,

- Business: 43.7%
- Health care/medical: 35.6%
- Education:7.7%
- Banking/credit/financial: 7.3%
- Government/military: 5.6%

Causes of Data Breaches

1. Weak and Stolen Credentials, a.k.a. Passwords

Hacking attacks may well be the most common cause of a data breach but it is usually a weak or lost password that is the vulnerability that is being make the most of by the opportunist hacker.

2. Application Vulnerabilities

Hackers enjoy to use the data from software application which are poorly managed or security system are poorly designed or implemented , they leave the hole from which they crawl straight to our data.

3. Malware

Malware is defined as a malicious software: software loaded without intention that opens up access for a hacker to peep in our system and potentially other connected systems. The use of malware can be direct or indirect with great success rate.

4.too many Permissions

As we use some web site,we have to go through the number of permissions and cookies ,we don't read many of them and we just accept or allow. Some of them might be the third party or hackers which we allow unintentionally and they get our data.

4. Insider Threats

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors,workers or business associates, who have confidential data concerning the organization's security practices, data and computer systems.

How data breaches occur?

1. Physical Theft and lose

Stolen or misplaced laptop ,phone or any paper document can make huge disaster for any organization. An foe gains a physical access to a system or a device through theft of the item.

2. Insider and privilege misuse

An disgruntled employee definitely knows the value of data that he can use it on shared device or any malicious intention. Insider misuse can be physical and virtual ,he can email the sensitive data or steal the data which can put the company's security at risk.

3. Crimeware

Crimeware also known as spyware is a software that designed to steal our personal and sensitive data and can be a social engineering attack . Through this they can easily get our online activities and other information.it includes

I)Ransomware

Ransomware is malware that employs encryption to hold a victim's information at ransom.
Specifically users files is encrypted so that they cannot access it,criminals hostages our file until we pay to unlock it but in most of the cases we don't get our file back.

II)SQL injections

SQL injections(SQLi) is a web security vulnerability that allows attacker to interfere the with the backend database,manipulation to access information which they can not retrieve without access permission. In many cases,they modify, alter or delete the data ,causing persistent changes to the application's behavior.

III)Phising attempts

Phishing is a type of social engineering attack in which the attacker acts as a trusted source and contacts the target through email, phone call, whatsApp, or SMS. The motto is to trick the target into installing malware or sharing personal information, such as bank account info ,credit card details or passwords.

4. Web application attack

Whenever ,we sign into new application we usually put our personal information but the serious vulnerability of application makes attackers to easily go through our data.

5. Payment card skimmers

Attackers can put the skimming device on a credit card reader and get our all the information through the device. This usually occurs at ATM or gas pump terminals.

6. Miscellaneous error

This type of attack to get benefit from vulnerable web servers by pushing cache servers or web browsers to reveal user specific information that might be sensitive and confidential.

7. Cyber - espionage

Cyber - espionage or cyber spying is the act in which unauthorized user get access to our ensitive data without holder's knowledge.This is a hostile email linked to state-affiliated actors.

What can offender do with the stolen data?

Take government benefit from your data.

Take tax funds.

Spam and unwanted marketing.

Blackmail and extortion.

Apply for credit cards and loans.

Distribute in dark web.

Phone scams.Transfer money illegally

Get medical care with your health insurance.

Prevention and precaution of data leakage,etc

Its very important to keep our guards up in order to safe data. These threat can cause serious damage to any individual reputation and can put the security on risks. We often give our data to web servers ,application and many more social activities ,we think that our data will be secure but these lightness sometimes make the blade up. There are many steps we must need to take which includes,

- Shred documents.
- Use safe and secure websites.
- Give Social Security number only when absolutely required.
- Create strong, secure passwords using uppercase and lowercase letters, non-sequential numbers, and special characters symbols.
- Use different passwords on every different account. This will minimize the damage if one of our account passwords is revealed.
- Must upgrade computers and mobile devices to the latest versions of operating systems and applications.
- Frequently monitor online transactions and monthly financial account statements to make sure transactions are precise
.
- Regularly check credit reports to confirm that identity thieves are not using credit card accounts or loans in your name.

Prevention to avoid data leakages,

1.discovering what kind of data stolen?

The data breach depends on the data which have leaked or stolen. Firstly we need to find how critical is the data. This means to categorize data based on their level of protection .If it takes the risk of your organization security , consider the penalty,inform the highers and take the help.

2.Using Encryption

encryption is commonly used to protect our data in transit or data in rest. Enabling encryption makes our data secure ,strengthen trust ,and protect our data even with the latest method of attack. Different encryption methods are based on the type of key size , key used , key length of data block encrypted.4 most common encryption methods are,

a.Advance Encryption Standard(AES): Advance encryption standard is a symmetric encryption algorithm encrypts fixed block of data at a time.

b.Rivest -Shamir-Adleman: it is a asymmetric method encryption algorithm that is based on the factorization of the product of two large prime number.

c.Triple DES: triple DES is a symmetric encryption and an advanced for of the DES encrypts blocks of data using a 56-bit key.

d.Twofish: twofish is a license-free encryption method that ciphers data block of 128 bit.

3.Lock down the Webwork

Locking down our webwork must be our primary concentration. Locking down your system or webwork means only you have the access to your content. It minimize the leakage risk and secure or social data. Lockdown network restrict the functionality of the system. Lockdown sytem need a password to access it makes easier even if we leave our work in between data breach risk will be very low.

4.Endpoint Security

Endpoint security is the practice of securing endpoints of end-user devices such as desktops, laptops, and mobile devices from being deed by malicious actors and campaigns. Endpoint security systems secure these endpoints on a network from threats.Organizations of all types are at risk from nation-states, organized crime, and malicious and accidental insider threats. Endpoint security is often seen as cybersecurity's frontline, and represents the first places organizations look to secure their networks.

DLP(Data loss Prevention) is a strategy that ensures end users do not share confidential or sensitive data outside of the enterprise network. DLP software solutions allow administrators to make rules that classify confidential and sensitive information so that it cannot be revealed maliciously or accidentally by unauthorized end users. DLP solution allows you to discover and control all sensitive data easily and identify at your risk users within seconds. These strategies involves a combination of user and security policies and security tools.

A **Data Activity Monitoring (DAM)** solution can provide another layer of protection by detecting unauthorized practice. While a DLP's focal point is on network and endpoints, DAM targets database activity.

Using both solutions concurrently provides broader protection through the layered use of monitoring and alerts, and blocking suspicious users or activities remotely.

III.Conclusion

Data leakage is the huge problem of growing world. Privacy and security is the right of every human being. Crime rates of data breaching is growing consistently every year. In this paper I have firstly explained what is data leakage and its type. Then I have explained the different threat that can be occur for any independent individual. Data security must be implemented to avoid any future anticipation. Even accounts that weren't breached might be compromised later, especially if we've been using the same passwords. Any suspicious behavior of our system can lead to leakages, threats and strict penalties. We must upgrade and check our devices constantly and avoid visiting supecios website that might use our data in mean way.

IV.References

1) Steve Symanovicih, a NortonLifeLock employee,What Is a Data Breach and How Do I handle one?

2)cyber edu: Data Leakage

3)Kris Lahiri, VP of Operations and CSO at Egnyte,Five ways to prevent data leaks

4)https://www.sutcliffeinsurance.co.uk