International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

HOW IS INFORMATION BEING LEAKED?

Yasaswi Vanarasi*, Sonakshi Sharma* & Dr. Zafar Ali Khan**

***Pursuing Bachelors in Data Science, Presidency University, Bangalore

**Associate Professor, Program Head - CSE, Department of Computer Science & Engineering, School of Engineering, Presidency University, Bangalore

ABSTRACT

As per a report by DataProt, 68 records are lost or stolen every second and news about data breaches becoming more common. Technology is advancing at an exponential rate. In this fast-growing environment maintaining security of data is highly crucial as a small loss of data might create critical impact in the organization, hence preventing their sensitive data became a greatest challenge. Traditionally organisations implemented methods like firewall, virtual private network(VPN) at the endpoints and framed control policies to mitigate the risk, but still these methods started lagging as the technology developed. The methodology of data leakage and data theft also attained heights. Hence there was a need for some system which could prevent leakage of data and this could be done with the help of Data Leakage Prevention system (DLPs). The DLPs are capable of detect leakage in Data at any states namely Data in rest, Data in transit and DSata in use which increases the need of the DLPs. This paper briefly discusses about concept of data leakage, reasons behind such incidents, various DLPs available & their limitations and related information.

INTRODUCTION

When confidential information is released to unauthorised individuals or parties, it is referred to as an information leak. Any casual examination of news sources reveals that data breaches occur with frightening regularity. Unsurprisingly, if information about project negotiations or tender information is leaked, your company may suffer a significant income loss.

Although information breaches may not appear to have a direct impact on your organisation, they frequently have indirect consequences. The loss of private client information can tarnish your company's reputation in the marketplace. Customers will be wary of collaborating with you or disclosing personal information to your organisation in the future.

CAUSES OF DATA LEAKAGE

Because data leaks enable data breaches, the causes of both occurrences are intertwined, hence the list below might pinpoint the sources of either data breaches or data leaks.

When monitoring attack surfaces, information security programmes should choose a data leak detection perspective to increase the effectiveness of data breach prevention efforts. This will inevitably reveal and fix the security flaws that are at the root of both cyber-attacks.

Managing vulnerabilities only for the sake of preventing data breaches narrows the threat detection field, increasing the risk of crucial data leaks. The following events are some of the leading causes of data leaks in 2021.

1. Misconfigured software settings

Software settings that are incorrectly configured might disclose valuable client information. If the leaky software becomes widely used, millions of people might be vulnerable to cyberattacks.

The Microsoft Power Apps data leak in 2021 was caused by this.

The data leak was first noticed by UpGuard on May 24, 2021. A major user data access setting was set to 'off' by default, leaving at least 38 million records vulnerable, including:

- Information about the employees
- Data on COVID-19 vaccine
- Contact tracing data for COVID-19

UpGuard researchers conducted a speedy repair reaction before thieves detected the data leaks by advising Microsoft of its exposure in a timely way. Millions of individuals and companies may have been victims of a broad cyberattack if this had not happened.

This monumental discovery demonstrates the catastrophic potential of overlooked data leaks.

According to Verizon's 2020 data breach report, software misconfiguration, such as those that caused the Microsoft Power Apps exposure and the 2021 Facebook breach, are on the rise.

2. Social Engineering

Cybercriminals seldom instigate data dumps, but when they do, it's almost always as a result of social engineering tactics.

The use of psychological manipulation in order to get sensitive credentials from victims is known as social engineering. Phishing is the most prevalent form of social engineering assault, which may be carried out orally or online.

A threat actor contacting an employee while impersonating an IT technician is an example of a verbal phishing scam. Under the guise of strengthening access in response to an urgent internal issue, the threat actor might seek login credentials.

3. Recycled Passwords

Because consumers prefer to use the same password for all of their logins, a single leaked password often leads to the compromise of many digital solutions.

Because stolen client data is commonly traded on dark web forums, this inadequate security approach results in a serious data loss.

Visit ‘Have I Been Pwned’ to see if your emails, passwords, or phone numbers were exposed in previous data breaches.

Multiple username and password combinations are used in a brute force attack. Even partial password information is categorized as a data leak because the remaining portion could be uncovered through brute force methods. Having partial password information decreases the number of required attempts, helping cybercriminals achieve success much faster.

4. Physical Theft of Sensitive Data

When company devices get into the wrong hands, sensitive information on them can be used to aid security breaches or identity theft, resulting in data breaches.

For example, a cybercriminal may use a stolen laptop to contact the IT administrator and pretend that they've forgotten their login credentials. The IT administrator will reveal this information with the correct persuasion techniques, allowing the cybercriminal to remotely enter into the company's private network.

The hacked laptop serves as the attack vector in this scenario, revealing data breaches that link the affected employee to the company's IT administrator.

5. Software Vulnerabilities

Software flaws, such as zero-day exploits, provide easy access to sensitive information. This skips the first step of a cyberattack, driving hackers straight to the privilege escalation stage of the attack lifecycle, the last stage before a data breach. These flaws might result in unauthorised access, malware assaults, social media account compromise, and even credit card fraud if they are exploited.

6. Use of Default Passwords

Even attackers have access to many of the factory-standard login credentials that come with new gadgets. As a result, factory-standard credentials that haven't changed are considered data breaches.

Such exposures have the greatest impact on IoT devices. When you buy these devices, they come with pre-programmed logins to help you get started quickly.

"admin" or "12345" are common login and password combinations.

Manufacturer instructions normally contain a strong caution to update these credentials before usage, yet this is a poor habit that both small businesses and major corporations have.

These data dumps might permit a large-scale DDoS assault since IoT devices are typically networked together.

In 2016, this is precisely what occurred. Kerbs, a cybersecurity blog, was the target of one of the greatest DDoS attacks ever recorded. The botnet that executed the attack comprised of 380,000 IoT devices that were seamlessly hacked through their default passwords.

TYPES OF DATA BREACH

1. Stolen Information

While this may seem absurd, humans are highly capable of making mistakes, and they do so frequently. Errors that might cost their organisation tens of thousands of dollars, if not millions.

A negligent employee at Apple even fell victim to this when a prototype of one of their new iPhones was left laying about. The specs and hardware of the yet-to-be-released phone were all over the Internet in a matter of hours.

It's all too usual for an employee to leave a computer, phone, or file somewhere they shouldn't and have it stolen. It might jeopardise not just the new prototypes you're attempting to conceal, but also customer or patient data.

2. Ransomware

When you receive a notification claiming that your phone or computer has been hacked, this is known as ransomware. In this situation, the individual will inform you that if you pay a price, they will hand it over to you and not reveal it to the public. This can range from a few hundred dollars to hundreds of thousands of dollars. Many businesses use risk management solution providers to prevent releasing or deleting sensitive or compromising information.

3. Password Guessing

When credentials are taken, another very simple but quite devastating issue arises. This occurs more frequently than you may expect. Some businesses leave computer passwords on sticky notes, allowing anybody to access them, perhaps allowing snooping employees to access information elsewhere.

Many people have their accounts hacked simply because their passwords were too simple or easy to guess. The term for this sort of breach is brute-force assault, and it is a highly popular tactic used by hackers. People frequently use passwords such as their street name, pet's name, or birthdate, which makes breaking into their accounts very simple.

It goes without saying that if someone knows your password, they may access your files and obtain any important information about your firm.

4. Recording key strokes

Keyloggers are malware that can record what you type on your computer and can be inserted or sent by cybercriminals. The information is subsequently handed back to the hackers, who utilise it to get access to critical information. This might happen at your workplace or on your home computer.

They record everything you type when this happens. Credit card numbers, passwords, and any sensitive information you could enter into a database, such as names, health data, or anything else, are examples.

This may be readily exploited against your organisation, since they will have access to your passwords as well as your firm's payment card information. They will then utilise these to obtain or leak sensitive corporate data.

5. Phishing

Phishing attacks are carried out by third-party hackers who construct websites that appear to be completely authentic. For example, they may create a site that looks exactly like PayPal and urge you to check in to make a necessary modification. You'll log in and discover that instead of merely checking in to your account, you've provided your password to someone else.

This scam is rather popular among institutions, and students may frequently get emails from a third party acting as the school, requesting confirmation of their login credentials. Once they do, the hacker gets their login credentials and may do anything they want with them. Phishing attempts have also been reported targeting Office 365 apps like Sharepoint and OneNote.

A phishing technique, once again, can jeopardise the security of everyone.

6. Distributed Denial-of-Service (DDoS)

This attack is typically only done to larger companies and is often a form of protest. For example, if vigilante justice trolls, like Anonymous, decide that they do not like the way a pharmaceutical company is running and feels it is taking advantage of patients, they can launch a denial-of-service attack.

With this type of attack, they will make it impossible for those at work to sign into the system. While the data isn't necessarily lost, they force the company to shut down while they deal with the security breach.

This type of data breach typically only happens to larger companies. It does not often happen to individuals, as it takes a very coordinated attack.

DATA LEAKAGE PREVENTION

Data leak prevention (DLP) is a term used to describe various technologies and processes used to identify, track, and protect sensitive data. The data leak prevention tools can include network security appliances, content-filtering software, and user activity monitoring tools.

Data leak prevention tries to detect sensitive data as it moves through an organization's networks and systems, and then take actions to secure it against unauthorised access or exposure. Accidental data breaches, hostile insiders, and foreign attackers looking to exploit exposed information may all be prevented with data leak protection systems.

11 WAYS TO PREVENT DATA LEAKAGE

1. Portable Encryption

Portable encryption is one of the most effective solutions to avoid data breaches. If you don't encrypt private information on your computer or device, it can be readily accessible. You can be certain that your data is safe and secure when you utilise portable encryption software, even if your device falls into the wrong hands.

2. Endpoint Protection

Endpoint protection software is another technique to avoid data breaches. This sort of software keeps track of everything that happens on your computer or device and protects you from dangerous threats or behaviour. You may help defend yourself from data breaches and other sorts of cyberattacks by utilising endpoint protection software.

3. Monitor Network Access

It's critical to keep track of every network access to avoid data breaches. You can help keep your personal data safe and secure by keeping track of who has access to it and what they do with it. You can simply monitor all network activity and safeguard your organisation from data breaches by using the correct tools and software.

4. Intelligent Firewalls

Another tool you may employ to avoid data breaches is an intelligent firewall. This form of firewall is designed to safeguard your computer or device from internet dangers including malware, viruses, and hackers. You can help keep your personal information safe and secure by employing an intelligent firewall.

5. Limit User Access

A good way to prevent data leaks is by limiting user access to sensitive information. By keeping a close eye on who has access to your confidential data and making sure they have a valid business reason for having it, you can help to prevent any unwanted users from accessing this information.

6. Assess Security Permissions

It's critical to revaluate security permissions when employees depart the firm. If an employee quits unexpectedly or returns on good terms but with changing duties, they may have access to sensitive data. When in possession of such sensitive data, you must ensure that permissions are changed appropriately so that they do not constitute a threat. If you're not sure, turn off all access and question them about any changes in responsibilities so you can both adjust to the new situation.

7. Evaluate all permissions

Examining all rights in your firm is a simple method to avoid data breaches. You can help keep your organisation secure from costly data breaches and other dangers that might harm your reputation or put you out of business by assessing employee access and choosing who should have what sort of access. Permissions should be evaluated on a regular basis, and access levels should be adjusted as needed.

8. Educate your employees

Make sure your employees are educated on the basics of information security and how to keep your data safe. Teach them about the dangers of phishing scams, malware, and other online threats. Regular education can help keep your employees aware of the latest security threats and how to protect themselves and your company's data.

9. Perform Regular Penetration Testing And Risk Assessment Audits

Regular penetration testing and risk assessment audits are another technique to lessen the chance of a breach. This guarantees that your data is secure at all times, even if your network contains any flaws or weaknesses that hackers may exploit. Penetration testing is hiring a third-party business with extensive experience in cybersecurity threats to examine your system for weaknesses or faults that might result in a data leak.

10. Maintain Up-To-Date Security Software And Patches

Finally, always make sure you're utilizing the most recent security software and fixes. It's the user's intellectual property and data protection key management method. You may lessen the risk of a data breach or other cybersecurity issue by keeping your software and systems up to date. It will also help to prevent data loss by providing backup services and keeping data safe.

11. Local scanning of data

In this method, an agent is installed on the host system that examines the content saved in the files on a regular basis. When it detects anything harmful in the material, it moves it, encrypts it, and quarantines it. Agents are constantly active during the process, executing a policy even when devices are not installed locally or connected to the network.

STATISTICS ON DATA BREACH/ LEAKAGE

- 45% of US companies have experienced a data breach
- The United States experiences the most data breaches of any country. In 2021, 212.4 million users were affected
- At least four 2020 breaches involved over a billion leaked records
- Companies that have experienced a breach underperform the market by more than 15% three years later
- In 2020, 50% of organizations spent only 6–15% of their security budget on data security.
- 58% of organizations don't acknowledge data breach disclosures
- 62% of companies in the Americas have experienced a data breach within the last year
- 28 percent of data breaches affected small business victims

DATA BREACHES OF TOP COMPANIES

1. Yahoo(2013)

- Records affected: 3 billion
- What was compromised: real names, email addresses, dates of birth, telephone numbers, and security questions
- Damages: $350 million estimated loss in value of company
- Who attacked: unknown
- Summary: Yahoo believes that "state-sponsored actors" compromised all of their users accounts between 2013 and 2014. It was difficult timing for Yahoo, as they were in the process of being purchased by Verizon, decreasing the value of the company by $350 million.

2. Facebook(2019)

- Records affected: 540 million
- What was compromised: phone numbers, user names, genders, and locations
- Damages: leaked account information
- Who attacked: no attacker
- Summary: Multiple Facebook databases were found to be unprotected by passwords or encryption, meaning anyone who searched the internet could find them. The databases cover multiple locations, including the U.S., the U.K., and Vietnam. Facebook announced in 2018 that it would make changes to "better protect people's information," yet this incident occurred in 2019, showing there were still flaws in their security systems.

3. LinkedIn (2012)

- Records affected: 540 million
- What was compromised: phone numbers, user names, genders, and locations
- Damages: leaked account information
- Who attacked: no attacker
- Summary: Multiple Facebook databases were found to be unprotected by passwords or encryption, meaning anyone who searched the internet could find them. The databases cover multiple locations, including the U.S., the U.K., and Vietnam. Facebook announced in 2018 that it would make changes to "better protect people's information," yet this incident occurred in 2019, showing there were still flaws in their security systems.

4. Adobe (2013)

- Records affected: 153 million
- What was compromised: debit and credit card information, usernames, and passwords
- Damages: $1.1 million in legal fees and $1 million to affected customers
- Who attacked: unknown
- Summary: In 2013, Adobe reported that nearly three million customers had their encrypted information stolen by hackers. Later in the same month, they raised their estimate to 38 million customers. A report that same week showed that more than 150 million accounts had been accessed. In 2015, a settlement was reached for violating the U.S. Customer Records Act and unfair business practices.

REFERENCE LINKS

https://www.titanfile.com/blog/case-of-confidential-information-leak/#:~:text=Primary%20causes%20of%20information%20leakages,accidentally%20sent%20to%20wrong%20recipients

https://internetbeginnertips.com/prevent-information-leakage/

https://www.upguard.com/blog/common-data-leak-causes

https://www.hubstor.net/blog/7-common-types-data-breaches-affect-business/

https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/#:~:text=The%20number%20of%20data%20breaches%20soared%20in%202021,down%2060%20percent%20from%202019.

https://ostec.blog/en/perimeter/understand-impact-data-leak/

https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time