5 Common Causes of Data Breach You Must Know

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/5-common-causes-of-data-breach-you-must-know/

By Liza Kosh | Published October 17, 2020 | Updated January 4, 2026 | Format: Analysis | 5 min read

In brief

The five most common causes of data breaches are physical device theft, weak credentials, human error, phishing scams, and application vulnerabilities.

A data breach is a frightening occurrence. It is an incident where information is accessed without authorization. Adobe, Dubsmash, MySpace, Yahoo, My Fitness Pal, faced some of the worst data breaches of the 21st century. These breaches affected millions of users.

Businesses not only face financial loss due to data breach but also lose the trust of customers and their reputation. With the advancements in technology, a lot of our information is on digital platforms. And because of that, incidents of data breach have become quite common. There are many causes of cybercrime; the top-most is that it is a profitable industry for attackers and hackers. Hackers steal personal information to compromise identities and steal money.

Let’s see the top 5 most common cause of data breach:

Physical Device Theft

When we think about cybersecurity issues, the first thing that comes to our minds is hackers working on computers in black clothes in dark rooms; that’s what we see in movies. But physical device theft is still one of the most common ways that lead to data leaks. People who are looking to steal your data can enter the premises and pick up unattended laptops and work their way to have access to all your company’s crucial data. To avoid breaches like these, it is compulsory to not leave devices unattended and they must be protected by password and refrain from sharing passwords with anyone.

Weak Credentials

Weak credentials are a major cause of a security breach. Weak passwords get stolen easily. When people use simple and predictable passwords such as "Password123", "123456", it becomes easy for criminals to have access to your data. In fact, they don’t have to work hard to get to know these easy passwords and attain sensitive information. Do you know that moderately secured passwords are not that secure?

They are in fact very easy to track by hackers by running computer programs through popular credentials. Whenever you choose a password, avoid the most common ones, and use a combination of alphabets, numbers, and signs. Oftentimes, we use the same password for different accounts; it is best to avoid this practice and avoid writing your password on a piece of paper.

Human Error

Human error is another reason that contributes to a data hack. You might be considering some bugs are the biggest reasons for a data breach, but data breach due to human error is quite common.

How human error aids in a data breach:

- Usage of weak passwords

- Using the same password for different accounts
- Sharing password with others
- Sending sensitive data to the wrong recipients

To prevent these human errors, companies should make sure that all employees practice the basics of data security measures. Training the employees and educating them can help in a significant manner.

Phishing

Through phishing scams, hackers acquire personal and confidential data. In Phishing, attackers send emails that look like they are from a genuine company. The aim of these emails is to entice the receiver to click on the malicious link or download the infected file so that attackers can gain the financial information of the receiver.

Application Vulnerabilities

No software is without technical vulnerability. Attackers take advantage of the situation and exploit it in different ways. Organizations are always working to find loopholes so that they can correct them before attackers discover them. When a vulnerability is fixed, the software provider releases a patch. The patch is supposed to be applied by the organizations that use the program. The process should be completed soon because when attackers are alerted to the vulnerability, they seek for organizations that are still exposed to the threat.

Malware

Security breaches are not always complex, and malware is a perfect example of that. Attackers buy malicious software and then look for a system that has a known vulnerability and plant the malware and exploit the data. Malware can be of different types; it can be the one that tracks every activity of the user or a one that locks the system and asks for payment to regain access.

Malicious Insiders

In an organization, many employees have access to sensitive data. You never know who can misuse the information. Malicious insiders sell the information on the dark web for financial gains. Sometimes, employees who are not happy working in the organization use sensitive information maliciously to hurt the reputation of the company. Make sure you protect your data from employees who didn’t leave on good terms.

How Can you Detect Data Breach?

Below we are providing some information that will help you detect data breach:

Data Breach Detection Tools

Data hacking is a serious issue. That’s why maintaining servers, systems, and applications are not enough; you need to have modern breach detection tools. Many organizations are still using old technology and compromising their data. It’s high time that companies start using modern technology to detect data breaching.

Monitor Attack Campaigns

When you use old malware detection products, they only allow you to see point-in-time threats, and alert you when individual events occur, which means people responsible for security have to chase a number of irrelevant alerts. Early detection can be done by organizations that pay attention on attack campaigns and not just individual alerts.

Regular Training to Staff

Oftentimes, the staff is not trained to prevent security breaches. Negligence on their part like weak passwords, leaving the systems unattended becomes a major reason for the security breach. All organizations should provide training to their employees on how to identify attacks and vulnerabilities. This training goes a long way in protecting organizations' data.

Stay up to date

Data leaks happen every now and then, attackers constantly evolve their methods; that's why it's important for organizations to keep evolving. Organizations should ensure that they remain up to date; they should be aware of the new attack methods and how to protect themselves.

Too Many Permissions

Permissions that are over the top and complex are a gift to hackers. Organizations should assess who has permission to access what within their organization. When organizations don't keep an eye, they give permissions to the wrong people.

Final Words

Data breach should never be taken lightly. Preventing data breaches helps protect your business and keeps your reputation intact. Hackers and attackers are always looking to exploit loopholes, make sure that your organization remains up to date to protect itself from malicious minds.

References

1. seasiainfotech.com - blog / worst-data-breaches-of-2020-tips-to-keep-your-business-safe - https://www.seasiainfotech.com/blog/worst-data-breaches-of-2020-tips-to-keep-your-business-safe/