**Data Breach**

Data Breach means accessing someone’s data without knowing them or without any authorization. Data Breach also called data leaking or information leaking. Data can be of any type it may be health-related data, can be business-related data, or any other sensitive data. Someone may be done intentionally or unintentionally and can use it to harm you personally or financially. Data breach now becomes a very popular attack in the field of hacking. Many growing hackers try these types of attacks to enhance their skills.   
A data breach can affect anyone in different ways of damage to down the company or someone’s reputation, and it can also affect the client of the companies.

**How Do Data Breach Happen:**

Data Breach happens when an attacker or cyber criminal tries to gain access and get success and can steal your personal information. It can occur in different ways like physically he can access your system by stealing it or by using it without your knowledge, or he can get access to your system through the network by providing any link or any file to your system which can help to gain access.

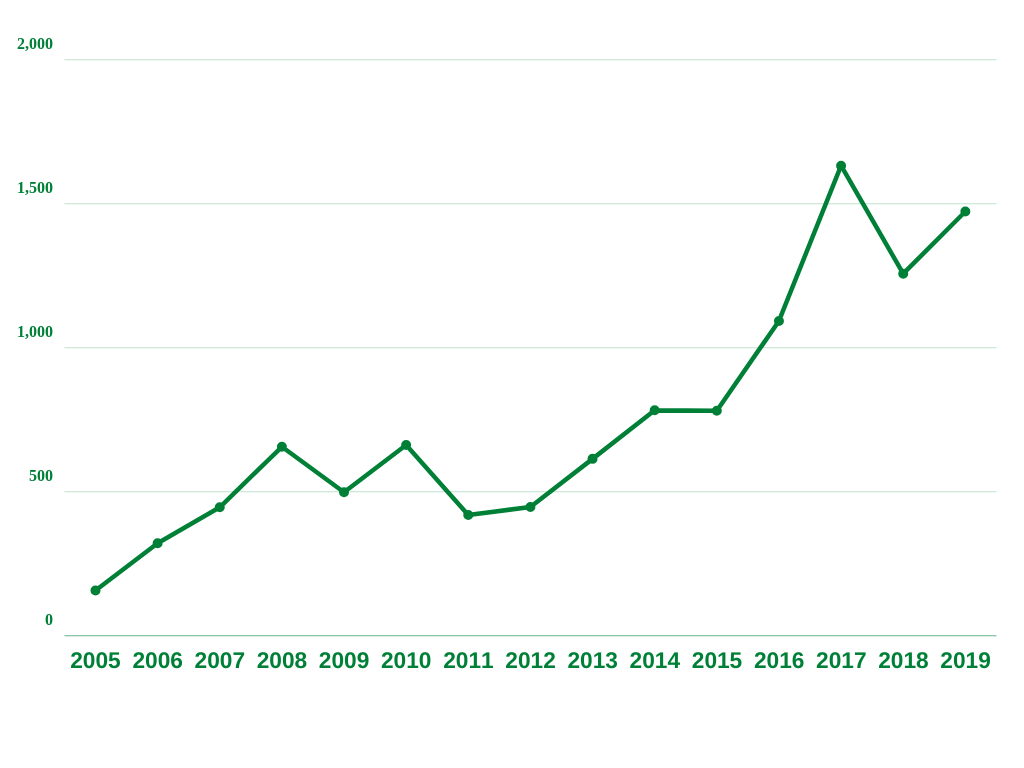
**Target Data:**  
Let us have a look at what is at stake if the data breach occurs:

1. **Personal Information-**  
   Some personal data or information get leaked like mobile number or email id.
2. **Credentials Fraud-**  
   Fraud in which data like bank details, card details get leaked by hackers.
3. **Stolen or theft-**  
   Sometimes mobile phones or laptops get stolen or theft this is also a cause of data breach.
4. **Third-Party access-**  
   We try to keep our system secure and protected, but sometimes attackers get a point to enter our system and can get our private information.
5. **Government Data-**  
   Many countries try to get access to other countries’ data or know about other countries’ plans so hires people for these purposes. To steal data like financial data, military data.

**Methods Of The Data Breach:**  
In this section, let us have a look at the different methods of the data breach:

1. **Ransomware/Malware-**  
   This type of attack has been increased since 2017. Basically in this type of attack, the attacker asks for critical information from the user or locks the system until the user paid the ransom for unlocking it. Example: Uber has paid attackers to delete the information of over 57 million peoples.
2. **Phishing-**  
   In these types of attacks, attackers generally fool the user to cause a data breach. Phishing attackers may be posses to be an employee or the organization you trust. They make you easily provide their sensitive data or gaining access to your sensitive data.
3. **Brute Force attack-**  
   In these types of attacks, attackers generally try to guess the password by finding all the possible ways to crack. They use hacking tools to perform these attacks. Sometimes it takes time to crack the password depending upon the strength of the password. If the password is simple then it can be cracked in seconds.

**Reported Data Breaches in the previous year:**



*Data Breach statistics*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Year** | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
| **Attacks** | 157 | 321 | 446 | 656 | 498 | 662 | 419 | 447 | 614 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **year** | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
| **Attacks** | 783 | 781 | 1093 | 1632 | 1257 | 1473 |

**Steps To Perform Data Breach:**  
Below are the steps to perform a data breach:

1. **Target Research-**  
   To perform the data breach the first step is to gather the information about the target so that it can help in further steps. These attackers gather information like how much they spend on cybersecurity, likes and dislikes of the target, hardware, and software used by the target. How secure the system
2. **Finding vulnerabilities-**  
   Whenever the attackers try to do the attack on the target the most crucial step is to scan the vulnerabilities. Vulnerabilities can play a role as a gateway for an attacker to gain access to the system and perform attacks. Hackers use many tools to find the missing port or any point to get into the system.
3. **Exploit the vulnerabilities-**  
   After finding the vulnerabilities attacker performs the exploit code on the vulnerability and enters the system.
4. **Injecting Payload-**  
   After successfully finding the vulnerability and exploiting it now attackers inject the payload to the system of the target. By injecting the payload now the attacker can have the valuable data he is seeking by entering into the system.
5. **Gathering Data-**  
   After injecting payloads the last and final step is to extract the required information. It can be either credit card information or it can be medical information or bank information or any financial information.

**What Data Breach Can Do:**

Data breach if occurs can cause a lot of damage. Below are some of the damages that can occur to levels of organization:

1. **Business Organization-**  
   It is very important for any organization to maintain their reputation and their financial bottom line but whenever the organization gets targeted the main thing which got targeted is reputation and their financial bottom line.
2. **Government Organization-**  
   When we talk about government information we are talking about military information, economic information, parties information, future plans of the country, and getting them targeted is one of the most dangerous things**.**
3. **Individual Information-**  
   When an attack is performed on an individual the information like credit cards, bank information, medical information, or any private information is at risk of getting leaked.

**How To Prevent Data Breaching:**

**For Enterprises:**

1. **Vulnerability Management-**  
   Using a vulnerability tool or at the very least complete a vulnerability assessment will help you identify the gaps, weaknesses, and security miss configurations within your physical and virtual environments. It can continuously monitor your infrastructure and IT assets for vulnerabilities and compliance weaknesses and configuration best practices.
2. **End-user security awareness-**  
   End-user security awareness training when done, is a huge benefit. But only when it changes the culture of the company to be more security-minded. Training insiders may help to eliminate mistakes that lead to the breach as well as notice odd behavior by malicious insiders or fraudsters.
3. **Update software regularly-**  
   Keep software updated, install patches, Operating system must update regularly as out-dated software may contain bugs that can prevent attackers to get access to your data easily. This is an easy and cost-effective way to strengthen your network and stop attacks before they happen.
4. **Limit access to** **your valuable data-**  
   In old days employees have access to all the data of the company. Now the company is limiting the critical data for employee access because there is no need to show financial data or personal data to the employees.

**For Employees:**

1. **Securing Devices-**  
   While using any device we should ensure that we have installed genuine antivirus, we are using the password on our device, and all the software is updated.
2. **Securing accounts-**  
   We should change the password of our account after a short span of time so that an attacker cannot get easy access to the account.
3. **Beware of social engineering-**  
   Whenever you are surfing on the internet be aware of fraud links and sites do not open any site or don’t provide any crucial information to anyone it can be so harmful.
4. **Keep checking bank receipt-**  
   You should daily check your bank transaction for ensuring that there is no fraud transaction.