TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

5

Ways to Keep Your **Organization Safe** from **Data Breaches**

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Data breaches have become so frequent now that it easily gets lost in our daily feed. Almost every single day, we are witnessing a plethora of data being exposed and published over darknet forums. Nearly 36 billion records were exposed in the first half of the year 2020 (Source: RiskBased). The consequences of such incidents are way beyond financial losses, damaging the brand's reputation and consumers' trust. high-profile data breaches, in recent times, have made organizations take a stand and put data security on top priority.

In this insightful information array, we will look at five effective ways on how to prevent data breaches.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

1. Vulnerability Management

Companies can mitigate the chances of a successful data breach by employing/outsourcing dedicated experts and tools for vulnerability management. Continuous monitoring of IT assets and security measures help in identifying vulnerabilities and misconfigurations, and fixing gaps before they are exploited by cybercriminals.

2. Regular Audits of Security Posture

As compared to vulnerability assessment & penetration testing, Security Audits thoroughly assess and validate the entire security policies of an organization by determining potential new gaps in compliance or governance.

Security audits may end up in common questions, like:

- Does your organization have documented information security policies?
- Do you have an incident response plan ready in case of security breaches?
- Do you have network security mechanisms in place (next-gen firewalls, IDS/IPS, EPP, etc.)?
- Do you have a security and log monitoring setup?
- Are there encryption and password policies?
- Are applications tested for security flaws?

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

3. File Usage & Access Policies

Illegal redistribution and imitation of sensitive corporate information are some of the major factors behind data breaches. It is important to understand that not every employee needs unrestricted access to your network, resources, and other critical assets. Enterprises must define file usage and access policies (can be done through Digital Rights Management solution) to get real-time visibility of data at rest, in transit and at work; limit access to critical data and restrict actions that can be performed by a specific user.

4. Multi-factor Authentication

Since threat actors have become more complex and advanced, businesses need to strengthen security by combining additional mechanisms with traditional methods. Passwords are no longer enough to keep accounts secure as hackers can sneak in using methods like phishing, brute force, dictionary attacks, etc.

One of the best ways to keep intruders away is Multi-factor Authentication. It complements existing security methods with additional features where logging in to a system or application requires entering a code, which is sent to your registered mobile number in the form of text. The best part is that the user will not be able to access the requested resource until the confirmation code is entered.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

5. Training to Employees

More than 90% of cyber attacks or breaches originate from Humans as they are the first line of defence. Hence, it is imperative for organizations to help them understand the basics of how to remain cautious while working and dealing with corporate data. Enterprises can consider training on the following:

- Usage of various, unique passwords on different systems and devices used for work purposes
- Implement a documented system for departing employees, vendors and contractors for passwords, key cards, laptop access, etc.
- Importance of reporting suspicious data security leakage or data security breaches
- Create a policy that describes how employees should handle, dispose of, retrieve, and send data

Towards The End

Threat actors may evolve and become more complex over time, but basics will remain the same for enterprises to be secure. Following proactive measures and implementing suggested controls can help organizations to prevent data breaches, as well as to safeguard the integrity of their sensitive resources to a great extent.