The Need for Data Security in Cloud Environment

While cloud computing is now extremely popular for the advantages it offers, data security continues to be a significant concern. Read this post to know the importance of data security in the cloud environment and what businesses can do to minimise the risks.

Cloud computing is one of the biggest boons to the world of technology in the last decade. Apart from data management and storage, it also makes it easier for people to access their data anywhere and anytime. Despite the benefits, however, threats to data security are real and compelling.

From customers having their data in the cloud to the cloud service providers, there are several risks concerning the security. Some of the most common ones include:

- Malware infections
- Permanent loss of sensitive data
- Account hijacking
- Violation of regulatory controls
- Insider threat
- Hacked interfaces

While there are several risks, there are also some effective means and solutions to keep your data secure in the cloud. Here are a few ways in which people can improve the security of their cloud data:

1. **Implement strong authentication tools**
   The time when a simple username/password combination used to do the trick is long gone. Modern hackers now have access to a host of advanced tools and technologies that can bypass the traditional authentication measures.

   A safer alternative is to use multi-factor or at least two-factor authentication to provide access to the data stored in the cloud. Add this authentication layer on top of the username/password to considerably improve the security of your cloud data.

2. **Data backup is crucial**
   Data backup is one of the most overlooked aspects of cloud computing. While the data will be available for you anytime and anywhere, it is still essential to take regular backup of your data. This precaution will ensure that you have a secure copy of your data stored in the cloud regardless of a mishap.

   Data backup is more about protecting your business and not the data stored in the cloud. Nevertheless, it offers peace of mind. You can take a backup in another cloud storage or an external storage device.
3. Employee training
From phishing attack and poor access control to misconfiguration, the majority of data breaches stem from human error. Such a possibility makes it critical for businesses to offer adequate training to their employees.

Provide your employees with the skills and information they would need for minimising the risks of unauthorised access and malware. They should also understand the importance of reporting potential incidents as soon as one is observed.

4. Off-board employees securely
When employees leave your company, you do not want them to take away your trade secrets. It is vital that you off-board them in a friendly and safe manner. It will help if you take away their data access to prevent data breaches, IP theft and other severe outcomes.

However, as employees often have access to many cloud applications, the off-boarding process is more complicated than it sounds. This further increases the importance of tracking who has access to your cloud applications. It would be best if you also had a detailed process with the help of which user access permissions can be easily revoked.

5. Monitor continuously
The authentication tools, staff training and backups are just the foundation of securing your cloud data. You also need to monitor the proceedings continuously and be vigilant at all times. Data encryption, monitoring data, tightly controlled access and identifying and resolving vulnerabilities are a few ways in which the security of the cloud data can be improved.

It is also imperative to continuously monitor the network and feed the latest details about potential threats. Flag any suspicious behaviour so that unauthorised access and malicious insiders can be uncovered.

Protecting cloud data amid rising security threats
Achieving adequate assurances on cloud security is possible only when you are ready to take a proactive approach to data security. Tata Tele Business Services (TTBS) offers MPLS (Multiprotocol Label Switching)-based VPN service with Secure Connect to provide businesses with a dedicated and private connection to leading cloud service providers such as Microsoft Azure and Amazon Web Services.

With the help of Secure Connect, businesses get a highly secure enterprise-grade network security to help prevent data breaches and further enhance the safety of their cloud data.