Overcoming Cloud Security Challenges

Cloud service refers to the collection of policies, procedures, controls and technologies, that work together to shield and cushion cloud based systems, data and infrastructures. Previously, we looked at some serious cloud security challenges and got to know how fatal they can be. Now, it is time to find how we can overcome those security challenges and increase strength of cloud security.

1. Data Breaches :

Preventing data breaches is one of the prime aim of every organization. It is consequential that data are safeguarded, preventing any sort of loss or contravention. To prevent data breaches, Cloud Security Alliance (CSA) recommends performing few key tasks such as encrypting data and defining data values. Furthermore, it is also equally important to have powerful and well-tested response plan.

2. Data Confidentiality :

Confidentiality of valuable data is the main reason why organizations implement cloud security services. With confidentiality, only authorized users can access the data making it safe and secured from mysterious users. To overcome issues related to confidentiality, it is important to implement information security protocols within multiple cloud layers. Furthermore, use of technologies like biometric encryption and HPI security can also boost confidentiality.

3. Misconfigurations :

Issues related to misconfigurations can lead to 80% of data breaches by 2025, according to Gartner survey (Common Cloud Misconfigurations and How to Avoid Them | UpGuard, 2022). Therefore it is important to avoid any sort of misconfigurations in cloud computing. To avoid misconfigurations, we need to have detailed knowledge about range of opening ports by

restricting unnecessary ports. Moreover, maintaining an inventory of company secrets and evaluating those secrets regularly can also minimize risks of misconfigurations.

4. IAM Issues :

The use of IAM has been growing as it provides essential et of tools, techniques and procedures to control access and resources. To ensure IAM support in cloud security, it is important to guide end-users about it. Errors are most likely to happen from the end user desk which lead in data loss or breaches. Appropriate attention must be given to cloud as an organization should determine IAM capabilities to find accurate designs and security measures.

5. Insecure Interfaces and API

To make sure that all interfaces and API are safeguarded and active, it is crucial for developers to practice a good API hygiene. It is said that API needs to be designed with encryption, authentication and activity monitoring. Developers should rely on standard framework and follow security protocols while designing API.

References

Common Cloud Misconfigurations and How to Avoid Them | UpGuard. (2022). UpGuard. https://www.upguard.com/blog/cloud-misconfiguration#:%7E:text=Cloud%20misconfiguration%20refers%20to%20any,vulnerabilities%20to%20access%20your%20network.