View on Web

How Businesses can Combat Risks of Cloud Computing

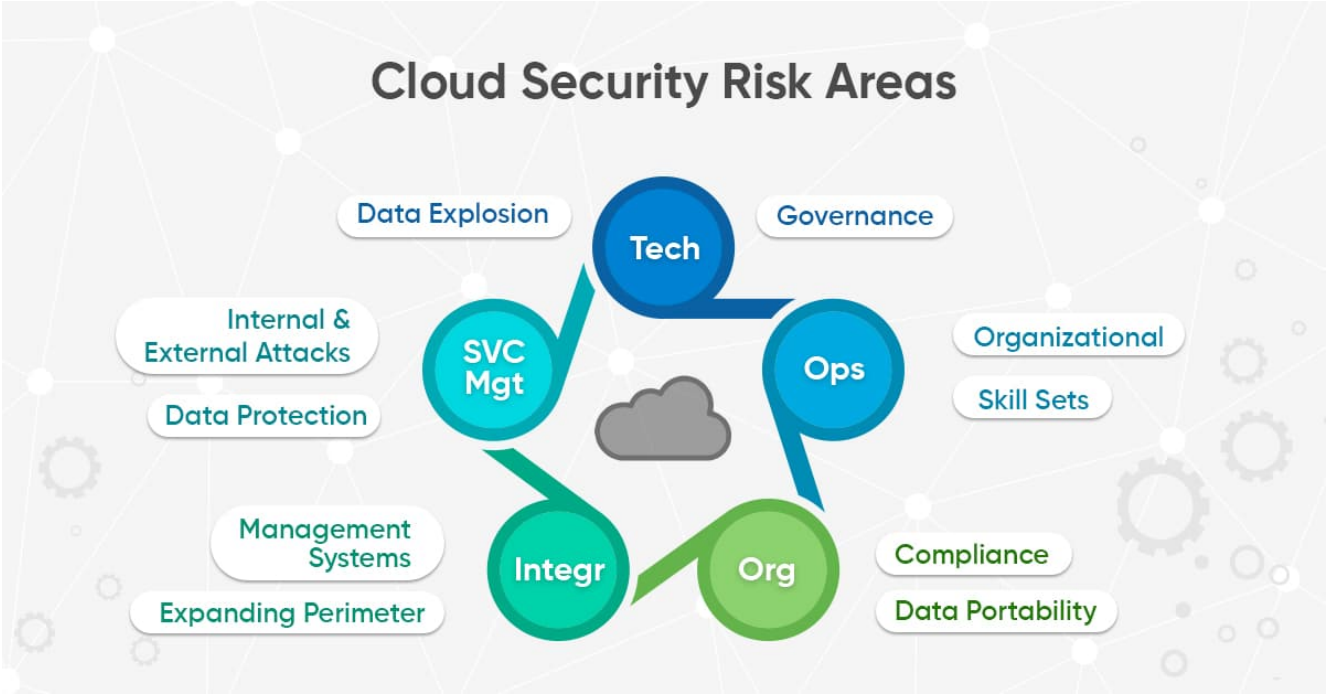
22nd Feb,2024

Cloud computing has radically transformed the way businesses access services from businesses. Just think how magical this serverless technology is! You don't need an on-premises server or storage device to access it. Unsurprisingly, more than 70 percent of businesses worldwide operate on the cloud. Cloud computing brings in a bunch of benefits-efficiency, flexibility, scalability, lower fixed costs, and more rewarding collaborative opportunities.

Despite a plethora of benefits, cloud computing is not immune to challenges. **The most formidable challenge is security. Plus, the emergence of multi-cloud environments and hybrid clouds has unleashed a novel set of challenges. Also, the regulatory environment for data is getting more stringent, which has amped up the compliance challenge.**

Cloud security hinges on its usage

Cloud service providers are heavily invested in the security of their offerings. They understand that if they don't secure their platforms, you simply won't use them. That's why they pour billions of dollars annually into ensuring that the technology they provide is as secure as possible. But here's the thing: it's not just about the service providers. It's also about how you use their services, how you structure your cloud solutions, and how your teams access cloud data. These factors determine whether your cloud security initiatives will succeed or fail. **According to Gartner, a whopping 99% of cloud security failures can be attributed to the customer's own mistakes. And if that's not enough, Gartner also found that 90% of organizations that fail to control public cloud use end up sharing sensitive data inappropriately.**



Dissecting risks and figuring out solutions

Data Breaches: Data breaches pose a colossal threat to your organization's **cloud security**. With the ever-increasing number of data breaches, more and more organizations are falling victim to the detrimental consequences on their reputation and finances. The regulatory and legal repercussions that follow these breaches only add to the woes. In today's digital landscape, data breaches have become the ultimate nemesis, lurking in the shadows, ready to strike at any moment.

Solution

- Encrypting all data, especially sensitive data with the most robust encryption tools
- Regularly performing data input and output integrity routines
- Removing, disposing of, or relocating data as per strict policies and procedures

- Putting in place a robust and proactive incident response plan to mitigate the damage in case of a breach

Inadequate Cloud Security Architecture: As hackers tirelessly refine their tools to exploit vulnerabilities, an organization's failure to establish a robust cloud security architecture can inadvertently pave the way for these cybercriminals. It's like leaving the front door wide open and inviting them in for a cup of tea.

Solution

- Restricting traffic between trusted and untrusted connections on the cloud and network environments
- Running regular risk assessments and making proactive changes in policies, procedures, and practices as required
- Implementing a continuous security monitoring procedure

Inadequate Access Governance: Just like other threats encountered by digital assets, cloud computing is highly susceptible to an organization's internal data access protocols that lack coherence. This vulnerability becomes particularly evident when it comes to an organization's overall cloud security and the sharing of sensitive data on it.

Solution

- Deploying Identity and access management (IAM) technology to manage users and access permissions. One form of IAM is when enterprises use Single Sign-On, giving employees access to all approved applications. Another example is Multi-Factor Authentication, which requires users to verify their identity across multiple devices.
- Running regular access privilege assessments and removing any unnecessary or unused credentials
- Timely modification of each employee's access to cloud, network, and data components based on their role and need to access these resources
- Documentation of all access control changes

Malware Injection: Malware continues to be an incredibly potent tool for disrupting an organization's operational protocols, particularly when it comes to cloud computing capabilities. Those with malicious intent are constantly seeking ways to compromise your organization's cloud security. One tried-and-tested method is by injecting malware-laden scripts into the very cloud services you rely on.

Solution

- Having a reliable enterprise malware removal
- Having a robust incident response plan to deal with any malware attacks

- Intrusion detection and prevention system that defends against malware, spyware, and other attacks

Insecure APIs: There are countless **Application Programming Interfaces (APIs)** out there, giving users the power to tailor and personalize their cloud environment. With their extensive usage, it's hardly shocking that these APIs are the most exposed elements of the entire cloud setup.

Solution

- Deploy APIs per the industry standards to ensure regulatory and legal compliance
- Avoid utility programs with the system, network, object, and application overriding capabilities
- Avoid reusing API keys
- Use open API frameworks

Cloud security is no walk in the park. It's not a "set-it-and-forget-it" deal. It demands your unwavering focus and attention, day in and day out. You can't just toss it aside and hope for the best. ***Businesses must be ever-vigilant, like a guardian angel protecting their precious data in the cloud.***

AUTHOR:

Jayajit Dash

Senior Manager- Corporate Communications (Marketing)