VIRTUAL TECH GURUS

CLOUD SECURITY AND BUSINESS RESPONSIBILITY

A WHITE PAPER

CLOUD SECURITY AND BUSINESS RESPONSIBILITY

Businesses should understand the different methods of security attacks and different areas of vulnerabilities within their organization.

When we hear about these attacks that have compromised user accounts on cloud services and SaaS (Software as a Service) providers, we want to know about the security infrastructure deployed in the data center of the cloud service provider.

One of the most challenging tasks is being able to protect the back-end systems of an IT organization from outside attackers. They can identify the vulnerability and can steal valuable data from the organization, which will result in major penalty to the organization regardless whether the hacker can be apprehended.

These kinds of remotely targeted attacks are executed continuously. What if the organization's data is compromised from the lost or stolen device? How do you address a situation where a malicious employee steals data from the organization before they exit company premises? How do you address a scenario where your employee accidently mistypes an email address which could result in sharing sensitive data with unauthorized personnel? What if a Virus or Malware infects the end-user's PC within the office premises and steals the data using session hijacking? If an organization does not scan files for viruses and malware before uploading them to the cloud, it can become nightmare for an organization.

These minor human errors can lead to major issues within an Organization.

In order to prevent these errors, our suggestion to an organization is to implement a Two-Factor authentication system which can be used to prevent future data apprehension from outsiders. Financial organizations have been using a powerful security method for many years in order to protect its sensitive financial data. They use fraud detection algorithms in order to identify unusual and inappropriate usage of accounts. The same method can be used by Cloud service providers. Encryption and Disaster Recovery tools can be used to help an organization prevent data theft or loss.

An organization should always be aware of what sort of security measures are implemented by the cloud service provider as well as from what point it should be able to monitor it's security activities on its own. Every organization should know what options they have available in order to strengthen their portion of security protocols. Organizations should author and distribute security guidelines for all employees, making sure those standard set of rules and regulations are met and followed verbatim.

IT departments of a company must ensure that only authorized personnel have the access to the company PCs and other devices. This will help businesses to run with less fear and more confidence.

For more information

Please contact your account manager or sales@virtualtechgurus.com

Virtual Tech Gurus, Inc.
5050 Quantum Drive, Suite 330
Dallas, Texas 75254 | 214.269.1314