

Ensuring Security in the Cloud - IO



Copyright © 2013 IO Data Centers



IO Blog



Ensuring Security in the Cloud

April 6th, 2010 / admin / 0 comments

SHARE 

Cloud computing promises scalability, continuity and cost benefits for businesses that decide to acquire “on demand” storage capacity, software applications and related services. Yet many businesses, understandably, remain wary of sending their data into the cloud, feeling that the practice could expose their critical information to unacceptable security risks.

A great deal of confusion surrounds cloud computing security. A quick Google search on the subject reveals plenty of contradictory opinions and insight, along with a hefty dose of hearsay. It’s a baffling situation that leads many IT managers to steer clear of the technology.

Cutting through all the Web chatter, it soon becomes evident that the only way to take advantage of cloud computing’s multiple benefits without placing data at unnecessary risk is to develop a strategy that will find definitive answers to the big security questions. Here’s how to get started:

- **Understand the cloud.** Learn how the cloud’s uniquely flexible environment affects information security. If you don’t understand how cloud computing works, you’ll never be able to protect the data you plan to send in to the cloud.
- **Think about the nature of your business.** Understand that cloud computing makes regulatory compliance inherently riskier and more complex. Therefore, a company in a tightly regulated industry, such as pharmaceuticals or financial services, will typically have different and more demanding security concerns than a company that’s subject to less stringent oversight.
- **Talk to the cloud vendor.** Don’t blindly assume that a cloud vendor will do everything possible to protect your data. Find out for yourself how the provider handles such key security issues as user access, data segregation, encryption technologies and investigative support (should your business find itself embroiled in a lawsuit or government probe). If you’re not satisfied with what you learn, look somewhere else. You should also ask the vendor if it is willing to comply with a security

audit.

- **Bolster internal security measures.** Analyze your company's own security technologies and practices, such as network firewalls and user access controls. Make sure that these safeguards are strong and will be able to mesh well with cloud security measures.
- **Know where your data will go.** The cloud can be a dangerous place. If you're not careful your company's valuable data could end up in a distant foreign location where data intrusion and privacy laws are lax or non-existent. Check with the vendor to see if it is aware of this issue and places any jurisdictional safeguards on its customers' cloud data. In any event, you'll want to talk with your company's legal counsel for advice on how laws and regulations will affect whatever information you send into the cloud.
- **Think about the unthinkable.** Security also means reliability and protection against external forces that could lead to lost data and/or an extended service interruption. Therefore, you'll want to look for a vendor that has taken steps to ensure 99.9 percent-plus uptime, has a strategy in place to deal with power service interruptions and equipment failures and isn't located in an area that's subject to natural calamities such as earthquakes, hurricanes, tornados or floods.

Finally, since cloud computing is a relatively new and rapidly evolving practice, you'll want to stay alert to changes in cloud technologies and methodologies that could impact your data's security.

Tags: cloud computing, cloud security

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: <abbr title=""> <acronym title=""> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

POST C



www.io.com