daisy.

Cloud security issues that every business needs to consider

Contents

Introduction

In amongst the hype surrounding cloud computing, there are often sceptical voices raising questions about the security of this type of IT platform.

While concerns over cloud security are often based on misconceptions, there are certainly real issues in this area which need to be addressed by businesses before adoption can take place. The idea that businesses that have questions about cloud security will not be able to find sufficient answers is a concern.

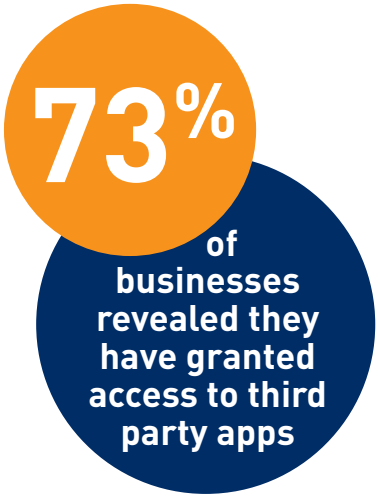
So what are the cloud security issues that every business needs to consider and are there ways to overcome any obstacles before their obstructive nature develops?

Voicing uncertainties

The areas of doubt expressed by businesses over cloud computing are useful in revealing where misunderstandings have arisen and where genuine weaknesses lie.

A study conducted by OneLogin and FlyingPenguin found that while 2013 will be the year in which cloud adoption pushes this type of technology into the mainstream, there are plenty of unaccounted for risks associated with using cloud apps in an enterprise environment.

71% of the staff questioned in the study said that they have in the past used cloud-based software solutions without the official permission of their company's IT department. Meanwhile, 73% of businesses revealed that they regularly have to grant temporary access to third party cloud apps in order to satisfy the usage needs of employees and external consultants.



Cloud vulnerabilities

Although many criticisms of cloud security focus on the ability of a third party provider to deliver adequate levels of protection for mission-critical apps and data, the real threats are far more mundane.

The OneLogin and FlyingPenguin study revealed that vulnerabilities of cloud apps are mostly down to the poor password choices and management of account information by individual members of staff.

43% of the businesses questioned revealed that employees keep passwords in unsafe locations, such as written down close to their workstations or saved to an unsecure spreadsheet.

34% said that passwords were being shared between co-workers so that they could log into business-specific accounts on social networking services like Twitter and even logistics platforms designed to handle courier requirements for the company.

Clearly this is a problem that should be addressed with training. Passwords which are easy to guess, simple to find, or end up being passed around among increasingly disparate groups of staff, are obviously not secure. This is true of any platform, whether it is hosted in-house or by a cloud provider.

20% of businesses said that they had suffered a security breach as a result of a former staff member still being able to log into a particular app or service after their employment had been terminated.

Report spokesperson Davi Ottenheimer said that this was an unacceptable state of affairs for most companies and one which should be easily corrected if companies take steps to prevent unsafe use of cloud apps.

OneLogin Chief Executive Thomas Pedersen said that the use of unsanctioned cloud apps is inherently problematic, although the answer to this issue lies in allowing IT departments to sanction a wider array of apps for enterprise use rather than putting yet more restrictions on staff.

Since the report found that many employees are willing to slip the bonds of what the IT department allows in the name of making their jobs easier, cracking down on these misdemeanours is less important than actually getting to the route of the issue and ensuring that cloud usage is safe no matter where it occurs.

43%
of employees keep passwords in unsafe locations

20%
suffer security breaches by former employees

Cloud strengths

It is important to remember in amongst all this, that the cloud is arguably a more secure place for a business to store its data and run critical apps than any on-site alternative. When a company is responsible for handling its own security and managing access internally, the burden of monitoring systems, updating protection and responding in the event of a breach is all placed upon the IT department.

If, on the other hand, a firm decides to outsource data storage and app operation to a cloud provider it will be able to free up resources, reduce costs and benefit from a scenario in which a dedicated third party is working around the clock to ensure the integrity of key IT systems. There may still be concerns over governance, although the study cited earlier shows that businesses should be more concerned about implementing strict best practices when it comes to passwords.

BYOD influence

One aspect of the report which needs to be examined closely is what it reveals about the growing trend for third party cloud app access from a portable device which is unsanctioned by IT departments. 80% of the employees who responded to the survey said that they had used a smartphone to access cloud apps while out of the office, with 71% relying on tablets for the same purposes and 80% downloading data remotely to computers not owned or operated by their employer.

An increasing number of companies are deciding to encourage mobile and remote working, which inevitably leads to staff members accessing enterprise data and apps from personal gadgets. The BYOD (bring your own device) culture is something which should arguably be condoned, if only because it is building up such momentum in the modern market that to fight against it is futile. However, this does not mean that companies need to have a completely complacent attitude towards how staff use their smartphones and tablets.

Instilling employees with the right attitudes about password usage, cloud security and access management, will mean that businesses are able to prevent unsafe approaches to cloud computing and foster an environment which can boost productivity without being detrimental to data protection.

Businesses need to be aware that no IT platform can be thought of as completely secure, particularly when the weak link is invariably the human user who accesses it on a daily basis. With this in mind, it is easier to allay fears about the usage of cloud apps and come at this technology from a positive angle, albeit one which also accepts that the legitimate concerns over security need to be tackled head on.

Businesses will need to rely upon the cloud to a greater degree as the pressures of data storage and processing capacity continue to grow, so it is worth embracing the totality of this type of service, including the benefits and potential pitfalls, in order to thrive in the future.