Five Security Must-Do's For First Time Cloud Users

What do Apple, Amazon and Microsoft have in common?

The answer: All three technology giants, considered the gold standard among cloud computing providers, have suffered the ignominy of being breached by hackers.

Apple's "celebgate" incident exposed personal photos of its celebrity iCloud users and made unwelcome news headlines last year. UK technology provider Code Spaces was forced out of business last year after hackers tried to blackmail it and subsequently deleted crucial data from its Amazon Web Services-hosted cloud storage. In 2013, an expired SSL certificate in Microsoft's Azure cloud service gave hackers the chance to bring down the Xbox Live and a raft of other cloud-hosted services.

Cloud security risks are rising, with attacks growing at 45% year-on-year globally, according to cloud security firm Alert Logic. In the next five years, US$2 billion will be spent by enterprises to shore up their cloud defences, according to Forrester Research.

First time cloud users can be most at risk, simply because of unfamiliarity with the new environment and the added burden of having to grapple with a new way of managing users, data and security.

Here are five security must-do's before taking the plunge.

1. Know the cloudy areas

There are three main segments in any cloud deployment - the cloud vendor, network service provider and enterprise. Given that the cloud should be treated like an extension of the enterprise data centre, the question to ask is therefore: can a common set of security services and policies be applied across the three segments? What are the security gaps?

During vendor selection, ask the cloud vendor what security services it provides and which security vendors it works with. The cloud is a dynamic environment and requires regular updates to the security architecture to stay up with the latest threats. How does the cloud vendor guard against

new security exploits and zero-day vulnerabilities?

Also find out where the boundaries are in the shared security models that come with the cloud service. Understand the extent of your cloud provider's responsibilities - and your own. In some cloud services, such as IaaS, it is the responsibility of the enterprise to secure its applications and data in the cloud. It is therefore important to know what security appliances and vendors the cloud provider offers/allows the enterprise to deploy in the cloud to do just that.

2. New apps, new fortifications

Ready to move an application into the cloud? Before you do, consider adding new fortifications to the existing security measures you have built around your application's authentication and log-in processes.

To fortify the access to your cloud application, you should have a granular data access scheme. You can do so by tying access privileges to roles, company positions and projects. This will add an additional layer of protection when attackers steal your staff's login credentials.

Account hijacking may sound basic but this age old breach has been flagged by Cloud Security Alliance as a continuing top threat for cloud users. To fortify your login process, consider implementing two-factor authentication, posture checking and the use of one-time passwords. A good tip is requiring user IDs to be changed at initial logins.

3. Embrace encryption

Data encryption is one of your biggest security ally in the cloud, and it should be non-negotiable when it comes to file transfers and emails. While it may not prevent hacking attempts or data theft, it can protect your business and save an organization from incurring hefty regulatory fines when the dreaded event happens.

Ask your cloud vendor about their data encryption schemes. Find out how it encrypts data that is at rest, in use, and on the move. To understand what data should be encrypted, it helps to get a handle of where they reside - whether in your cloud vendor's servers, the servers of third-party companies, employee laptops, office PCs or USB drives.

4. Wrestling with the virtual

Moving into the cloud lets businesses reap the benefits of virtualization, but a virtualized environment can present challenges to data protection. The main issue has to do with managing the security and traffic in the realm of multi-tenancy and virtual machines.

Physical security appliances are typically not designed to handle the data that is in the cloud. This is where virtual security appliances come in - to secure traffic as it flows from virtual machine to virtual machine. Such appliances are built to handle the complexities of running multiple instances of applications, or multi-tenancy.

They therefore let businesses exert fine security control over their data in the cloud. Ask your cloud provider how it safeguards its virtual environment and find out what virtual security appliances it is using. If you are building your own private or hybrid cloud, consider getting virtual security products that focus on granular control.

5. Don’t be in the dark about shadow IT

There is no shortage of anecdotes and reports out there that point to how the unauthorised use of applications and cloud services, or shadow IT, is on the rise among businesses. The uncontrolled nature of this poses a security threat and governance challenge.

Your new cloud application will be at risk because of this. Consider the simple scenario in which your employees use their smartphones to open a file on their device. It is likely that the phone will make a copy of the file, which could then be sent to an unapproved online storage destination when the phone does its routine automatic backup. Your secure corporate data has just been moved to an insecure location.

Preventing access to shadow IT is unlikely to stop its growth in any given organization. It is more effective to educate your users and use technology to manage the issue. Encryption, network monitoring and security management tools can help defend your first cloud app against the risks of the shadow IT.