Public cloud security in the post-PRISM era

George Orwell's novel 1984 described a world dominated by big brother governments using their powers to spy on citizens. Although it was a chilling, dystopian view of life, the book resonated with early readers and many of them came to the conclusion that this abuse of power was not only possible but actually happening during the Cold War.

Covert espionage is still an issue today. With the advent of new technologies such as public cloud computing, it's easier than ever for governments and criminals to hack into personal data and glean information. The recent press coverage surrounding the US government's PRISM scheme and the intrusive snooping by other foreign institutions proves this point. It comes as no surprise therefore that more people and businesses alike are getting worried about the security of cloud. Should any data be stored via the Internet? Are we making it easy for security breaches to occur? Does this spell the end of cloud computing as we know it?

Public cloud continues to grow in popularity, despite any fears reported by the press. Some of the biggest companies in the world are already using it for storage, such as Amazon and BT, and they aren't changing their business models anytime soon. Dropbox, one of the world's most famous public cloud storage platforms, announced just weeks after the PRISM scandal broke that it was broadening its reach with the launch of Datastore API. Far from offering more protection to shield data, developers will now be able to sync structured data not normally accessible for file synchronisation. In other words, Dropbox is blurring the barrier between app, device and OS. Sharing and transferring data has never been easier.

The growing popularity of Dropbox is truly extraordinary. The company has attracted 175 million users - up from 100 million less than a year ago. That number is also expected to increase as more individuals and companies look for ways to manage their files. Even organisations that store highly sensitive data are investing in public cloud services like Dropbox. A good example is healthcare providers such as the NHS, which use cloud to host personal medical data to cut costs and increase storage capacity.

For many sectors, the advantages of the cloud seem to outweigh the big disadvantages that increase risk. These weaknesses include the lack of knowledge surrounding where servers are located. They might be in countries that are politically insecure or prone to natural disaster - both of which can threaten safety of data. Also, data is shared publicly, which makes it vulnerable to attack. Look at the ease with which PRISM conducted its global campaign of espionage. Furthermore, data isn't usually encrypted on the cloud, so if there's a malware, virus or hack attack, it can be lost forever.

PRISM worries aside, the drawbacks of using public cloud are often ignored by companies for the sake of its benefits – and there are plenty of those. A big perk is public cloud flexibility in accessing applications anytime, anywhere. Organisations that may have limited access to servers or don't want to have them on-site might prefer to use public cloud too. Those with large numbers of remote workers or a highly mobile workforce also find it beneficial.

This all sounds great, but if companies decide to use public cloud they should also understand that data is at risk and any sensitive material should be encrypted to add an extra layer of protection from attacks and data disasters.

It's important to remember that a lot of data up in the cloud isn't that sensitive to warrant widespread panic. Companies that have reason to worry-like financial services institutions and government organisations - are staying clear of public data storage too.

Furthermore, the biggest threat to company data will always come from within an organisation. The fear of being hacked by the government or an elite, IT savvy gang of fraudsters is extremely small for most businesses. Over 90 per cent of the greatest risks to data - such as malware, viruses and hacking - are done by people opening malicious attachments, taking things away on a USB or downloading them into personal devices.

With this kind of low-tech, internal hacking, you can't avoid the problem by simply installing a piece of software or moving something out of the cloud. Companies have to introduce security processes and find ways to implement them effectively.

Whether it's a whistleblower or a rogue employee set on stealing data, in most cases, the most disruptive cloud crimes will almost always be an inside job. This is risk that's most often overlooked - and sadly, there's very little that can be done if an attack occurs and there's no security plan in place.

Richard Eglon
Marketing Director, Comms-care
reglon@comms-care.com
@richardeglon