BIZCOMMUNITY

Safe cloud computing starts with sound information security practices

By Sumash Singh

22 Jul 2015

The move toward cloud computing services is gaining traction across many industries due to rapidly growing volumes of data that require storage. For the security sector, surveillance footage is the biggest demand on storage, and as the resolution of security cameras continues to increase, so too does the storage requirement. In addition, for this footage to be useful it often needs to be stored for extended periods of time. As a result, security organisations are increasingly looking toward the cloud to meet their storage requirements.

However, it may not be appropriate to store surveillance footage and other business-critical data in a public cloud scenario, as this could potentially open the organisation up to risk. Choosing the most appropriate cloud model, be it public, private or hybrid, is an important decision, and understanding what data organisations have, where it resides and how valuable it is to the organisation is critical. Implementing sound information security practices is, therefore, essential before embarking on any cloud migration, to ensure that the necessary data is protected in the appropriate manner.

Hybrid cloud becoming go-to standard in South Africa

When selecting a cloud service provider, the value of the information to the business is the first and most critical factor. Mission-critical, confidential or sensitive data should ideally be carefully thought about, before being entrusted to a public cloud provider, as the potential risk of exposure is too high. On the other hand, data that is less critical or sensitive can be stored in the public cloud for the business benefits of agility, flexibility and cost effectiveness.

Impending legislation such as the Protection of Personal Information (PoPI) Act means that organisations are beginning to place more importance on how information is stored, disseminated and distributed between various sources. As such, organisations are also looking more closely at secure, enterprise-grade cloud infrastructure.

The hybrid cloud has thus become the go-to standard in South Africa, with organisations blending together on-premise private cloud solutions for certain applications and services, and extending other applications to delivered out of the public cloud service providers.

pixelcreatures via pixabay.com

The unknown and uncontrolled

In South Africa, many local service providers are delivering this type of solution, enabling organisations to make use of cloud services while still maintaining data sovereignty requirements by keeping the information in the country. The challenge to overcome here is that while the organisation itself may have a defined hybrid cloud strategy, employees within their organisation may already be making use of public cloud services such as social media and peer to peer data sharing and storage solutions.

The unknown and uncontrolled use of the social and peer to peer solutions represent a more significant risk as they potentially expose confidential data to public cloud providers, which are not governed by the organisations compliance and data retention policies. As a consequence organisations frequently discover that valuable business information resides outside of the controlled perimeter of their private or hybrid cloud.

Organisations need to understand how much of their information is unsecured, and then adopt an appropriate strategy and technology to bring this back into the corporate infrastructure, under the corporate compliance rules. While there many advantages to the public cloud, organisations, particularly those in the security space, need to exercise caution over what

information they have willingly chosen to expose to an environment such as the public cloud. It is essential to bear in mind the type of data an organisation generates, the value of this data and the reputational or business impact should that data be exposed.

The basic underlying premise of PoPI

Information is the central component of a cloud strategy. If the information is critical to the reputation or Intellectual Property (IP) of an organisation and requires layers of protection, then this characteristic dictates the type of cloud infrastructure it is suited for. However, the value of information also has a specific lifecycle and diminishes over time. It cannot simply be kept indefinitely in multiple data sources without organisations knowing exactly where it is, and when it could be defensibly deleted. This is the basic underlying premise of PoPI.

Organisations first need to identify all of the places their data resides and classify it according to its importance to the organisation, aligned to corporate policy. It is also essential to understand who has access to the data, and the level of access they have. Legal requirements, such as how data is governed and the policies behind this also need to be considered. Information management principles guide security, and thus must be implemented before data is moved into the cloud, off-site, off premises or even offshore. Information security management is critical to ensuring safe cloud computing practices.

ABOUT SUMASH SINGH

Country manager at CommVault
- CIOs vs. consumer technology: it's time to change strategy - 6 Oct 2015
- The rise of the chief data officer - 1 Oct 2015
- Designing a cloud that meets your business requirements - 7 Sep 2015
- Safe cloud computing starts with sound information security practices - 22 Jul 2015

View my profile and articles...