Steps to securing cloud data

By Neil Cosser

1 Nov 2018

Leadership is essential when it comes to ensuring the security of data stored in the cloud.

Neil Cosser is identity and data protection manager for Africa at Gemalto

Cloud adoption in key African markets has grown phenomenally over the past five years. According to a recent study by World Wide Worx, it is pervasive in the key African markets of South Africa, Kenya and Nigeria, with between 95-100% of medium and large companies using the cloud.

Eighty percent or more of companies in these countries will increase their spend on cloud computing into 2019.As a result, growing amounts of sensitive customer (and company) data is stored on the cloud, and there is evidence to suggest that many organisations are still struggling to secure their clouds.

Six months into 2018, some spectacular breaches had occurred, with the most significant being the personal information of all 1.1 billion citizens registered in India. Locally, the most significant case has probably been the breach at Liberty Holdings in January. Such breaches are increasingly common.

Non-compliance: leading organisations down the rabbit hole

Simeon Tassev 10 Oct 2018

A complicating factor is that businesses often operate across more than one cloud, such as AWS and Azure, each having differing security protocols to grapple with. Worse, many appear to be reluctant to even address the issue at hand.

The 2018 Global Cloud Data Security Study, conducted by the Ponemon Institute on behalf of Gemalto, shows that a third of respondents (34%) believe that it's the customer's responsibility to secure their data in the cloud, whereas two thirds (62%) of customers actually hold businesses responsible. With less than half (46%) of businesses clearly defining roles and accountability for securing confidential or sensitive information in the cloud, it's clear many are struggling to get their houses in order.

Global study finds AI is a key cybersecurity weapon

28 Sep 2018

Taking responsibility for cloud security

In a growing number of countries, the legal responsibility for safeguarding customer data, no matter where it is housed, is unambiguously allocated to the company or organisation. The General Data Protection Regulation (GDPR) in the European Union and the Protection of Personal Information (PoPI) Act in South Africa are just two examples of this growing international trend.

Organisations, and ultimately their boards, found to be taking insufficient steps to secure the data will be subject to fines and legal repercussions. So, what can organisations do to avoid falling foul of both regulators and customers?

The key ingredient is leadership. While cloud services themselves are generally secure, the task of configuring and using them securely is often left to organisation's IT leaders, development teams, or even business line managers. However, confusion surrounding who should implement cloud security has created challenges. Organisations must now take full ownership of the security within their clouds. A figure, such as a CISO, must be appointed to the board of a business to educate other C-level executives on the importance of data security and take responsibility for the data in the event of a breach. This ensures the business has buy-in from the board, can communicate a cloud security strategy widely, and educate staff about good cyber hygiene, thus minimising internal risks.

Why are CIOs and CISOs positions becoming more challenging?

Pieter Engelbrecht 31 Oct 2018

Once a central figure has been appointed to the board, he or she must set about ensuring that the cloud is protected. Below are five steps to help with this.

Five steps to cloud security

1. Understand where the data is

1. Understand where the data is

Before implementing any cybersecurity strategy, businesses must first conduct a data audit. This helps them understand what data they have collected or produced and where the most sensitive and valuable parts sit. If businesses don't know what data they possess and produce, they can't even begin to start protecting it.

- ## All sensitive data must be encrypted

While it's crucial that businesses restrict who can access sensitive data, it's encryption that protects data in the event of a breach. Regardless of where data is – on their own servers, in a public cloud, or a hybrid environment – encryption must always be used to protect it.

- ## Securely store keys

When data is encrypted, an encryption key is created to unlock and access encrypted data. Consequently, businesses must ensure that these keys are securely stored away from the cloud. Storing a physical key offsite helps ensure it can't be linked to any encrypted data in the cloud.

- ## Introduce two-factor authentication

Next, businesses should adopt strong two-factor authentication, to ensure only authorised employees have access to the data they need to use. Two-factor authentication involves using something authorised individuals possess, such as a smartphone that can receive a message, and something they know, like a password. This is more secure than relying on passwords alone, which can be easily hacked.

- ## Always install latest patches

As bugs and vulnerabilities emerge, hardware and software vendors constantly issue patches. However, many businesses don't install patches quickly enough or use software which no longer receives regular patches. Figures from Net Applications show that one in 10 organisations still use Windows XP, despite patches being discontinued. It is imperative that businesses install patches as they become available, to avoid becoming easy targets for hackers.

- ## Evaluate and repeat

Once a business has implemented the above steps, it's crucial that each step is repeated for all new data that enters its system. Cybersecurity and legal compliance are a continuing process, not an event. These steps will ultimately help make businesses unattractive or unviable targets for attackers as even in the event of a breach they won't be able to use, steal or hold their data for ransom.

With businesses now footing the bill, reputationally and financially, for any data breach, it's never been more important for them to take full ownership of the data they hold.

ABOUT THE AUTHOR

Neil Cosser is identity and data protection manager for Africa at Gemalto