Data security in the cloud - whose responsibility is it really?

When moving data into the cloud, organisations should be aware that it is the responsibility of the information owner to ensure that holistic protection and clear visibility is in place, to avoid security breaches.

Source: pixabay.com

Riaan Badenhorst, general manager at Kaspersky Lab Africa, says, “The desire to gain the many benefits related to the cloud, such as flexibility, cost savings and increased efficiencies, has led to most enterprises moving an increasing amount of data to the cloud. However, as the quantity of data residing in the cloud increases, we find that the organisation's clarity around potential threat levels of data exposure decreases. This can ultimately lead to unpleasant consequences such as cybersecurity breaches, if not correctly managed.”

Where is the cloud?

Bernard Ford 13 Aug 2018

Kaspersky Lab recently released a report entitled ‘Cloud Zoo: Don’t Let Your Business Data Roam Free’, which indicates that 59% of small and medium businesses (SMBs) and enterprises feel that outsourcing and cloud hosted services could introduce new risks to the IT security of their business.

Yet, despite such concerns, nearly half of businesses still do not take cloud security seriously, where at an enterprise level, 42% of businesses admit they are unsure where certain parts of corporate information is stored, making it difficult to account for its integrity.

“A large portion of this uncertainty arises due to the concept of ‘shared responsibility’. Outsourcing to a cloud provider is one thing, but most often, the service level agreements state that the service provider only covers 'service availability' and 'security of the cloud infrastructure'. What this often presents is confusion in the responsibility of data protection in the cloud. The reality is that data that is affected in the cloud – whether its credentials are compromised, a ransomware attack occurs or some other form of data breach – is ultimately the responsibility of the customer,” adds Badenhorst.

What every business owner should know about migrating to the cloud

Aaron Thornton 3 Aug 2018

The consequences of failing to take responsibility of data in the cloud can prove to be financially significant for business. The report indicates that 41% of enterprises suffered an average loss of $1.2m as a result of cloud-related security incidents, while 46% of SMBs suffered damage amounting to around $100,000.

> *“It is therefore imperative that organisations are made aware of their own responsibilities in regard to cloud security, and that they understand just howimportant it is to map where their data is stored. To circumvent this and minimise a situation that can leave a business unsecured, unprepared and potentially falling victim to cyberattacks, businesses must look to equip themselves with a security offering specifically designed for effective cloud protection.”*

The value of the data in the cloud is such that businesses need to ensure they have holistic protection and visibility across all cloud platforms they use – to minimise the cloud melting cybersecurity perimeters. This can be achieved by crafting a well-balanced blend of best-of-breed protection, resource efficiency and enterprise-level orchestration capabilities for public and private cloud environments.

“Considering how much valuable data is stored in the cloud today, it has never been more critical for companies to ensure they have both protection and visibility across their cloud platforms. The cloud is designed to help businesses reduce their total cost of ownership as well as simplify operations and increase business agility – it should not add to their security concerns. Yet, a lack of understanding linked to the responsibility of data security in the cloud can leave a business in a vulnerable position – where the risks will outweigh the benefits,” concludes Badenhorst.