4 misconceptions about cloud security

By Christo van Staden

14 Sep 2018

The widespread adoption of cloud solutions has been driven by the myriad of associated benefits offered, such as flexibility, scalability and remote access.

Christo van Staden is regional manager: sub-Saharan Africa at Forcepoint

At the same time, concerns have been raised regarding the security of these solutions when it comes to keeping sensitive data safe from malicious actors. Many organisations take the easy way out and continue to work with their old, trusted IT infrastructure and as a result, play it safe with proven on-premise storage methods conferred by legacy IT infrastructure.

Moving to cloud? Take note of common security needs

Anton Jacobsz 4 Sep 2018

However, trust in the cloud has improved and many security concerns have been addressed by security vendors and cloud providers. Companies now utilise cloud solutions (whether a hybrid or pure cloud) to store their data and applications. But despite the fact that security has become much better, companies should be aware of the half-truths and myths that exist regarding cloud security.

Here are four misconceptions about cloud security providers at a glance:

- ## Cloud security providers do not need to present a security certificate

Compliance teams tend to only check certificates within their own organisation and extend them where necessary.

However, every partner - including the cloud security provider - must also have the correct certificates. This means that companies should request the appropriate certificates from providers before one is appointed. Failure to produce the correct certificates should raise concerns about how the provider processes and protects sensitive data.

For example, if an ISO 27018 certificate is missing, it is unclear whether a provider deals with personal data in the right way, which raises a red flag regarding General Data Protection Regulation (GDPR) compliance or Protection of Personal Information Act 4 of 2013 (POPIA).

Another tip is to have the control done by an external party. Such an audit requires time, energy and money, but some cloud security providers are unable or unwilling to make this investment. This is another factor that should be considered during the selection process.

What's holding SA back from the public cloud?

Johan Scheepers 6 Aug 2018

- **Data centres of cloud providers are always better secured than their corporate counterparts**

Cloud service providers like to point out the shortcomings of private data centres to show that their own cloud solutions are better protected. This is not always true. Although the cloud does indeed offer significant security benefits, it is the providers that need to take action to ensure that we actually benefit from these benefits.

It is not so much the infrastructure, but the extra security steps that security managers take - private or not. It is also not the case that a provider with the right certificates takes on all aspects of security. Most cloud service providers work with a shared security model. This means that the responsibility for user behaviour, accessibility and terms of use lies with the client, and not with the cloud service provider.

- **The more data centres a cloud service provider has, the better the performance and resilience of the infrastructure**

Although a cloud solution must have multiple data centres, it is not self-evident that the amount of data centres affects performance. For example, Microsoft Azure, which has only 30 data centres worldwide and works well. Other services with hundreds of data centres cannot always match Azure.

So while global coverage helps to reduce latency, cloud peering (creating a stable, private and direct connection between your own and public cloud) makes the difference when it comes to a good user experience.

- **The security of the cloud service provider itself does not affect the costs of cybersecurity insurance**

Insurance companies will review a company's cybersecurity posture in order to determine monthly premiums. If a company is deemed to not be doing enough, then this can affect the monthly amount.

Fortunately, this can be avoided by demonstrating that both the organisation and the provider are committed to optimum cybersecurity, by investing in adequate prevention of cyber threats, good data security and data protection.

Growing cloud security

More and more companies are seeing the benefits of working in the cloud, including better data security and accessibility for all employees, especially with regards to remote and mobile working. Cloud solutions also offer a degree of flexibility and scalability that surpasses legacy technology.

As a result, cloud-based security services will also continue to grow, reaching $9bn worldwide by 2020, according to a study by Gartner. For most companies, the cloud can and does have real business benefits - increasing efficiency, scalability and driving growth across markets. Knowing how to choose the right cloud security provider, therefore, remains important.

ABOUT THE AUTHOR

Christo van Staden is regional manager: sub-Saharan Africa at Forcepoint