More companies are favouring managed IT security services

By Richard Broeke

16 Mar 2015

More South African companies are beginning to favour managed IT security services. Where companies once considered it risky to hand over the function to a third party, keeping security in-house is proving to be riskier.

Richard Broeke

Why? The average business simply doesn't have the necessary skills and resources in-house to manage the constantly evolving, and increasingly sophisticated, IT security risks.

Gartner has predicted that, by 2018, more than half of organisations will use security services firms that specialise in data protection, security risk management and security infrastructure management to enhance their security postures. This will be driven by the lack of appropriate skills to define and implement appropriate levels of control.

Managed security services

Like with rest of the world, this lack of skills is already leading South African companies to adopt managed security services. Email, which is one of the focus areas for companies, is one of the aspects of IT security that local companies are becoming increasingly comfortable with outsourcing.

In the past, the uptake of Securicom's email security services was primarily around pure anti-spam and virus protection. In 2013, companies started focusing on more comprehensive solutions that not only provide security but data loss prevention, archiving and business continuity as well.

The uptake of MailVault, an email archiving and business continuity solution, and Securicom e-Purifier, a comprehensive email security and content management system, services that have existed for more than 15 years, continue to grow by over 30% annually.

Taking a managed services approach has potential to reduce the administration, complexity, and overheads of IT security significantly. Importantly, companies are better placed from a security standpoint because there is someone qualified managing the services and making sure they are up to date.

Historically, companies felt compelled to select and purchase security technologies with all the latest features despite not having the proper resources to use all those features effectively, or ensure that updates are correctly and regularly applied.

Various point solutions were commonly deployed to address different threats, but these solutions haven't been adequately managed or monitored. The result is that companies never had an accurate picture of their IT security status because this picture is constantly changing.

Costly to buy and maintain

It is also costly to buy and maintain various solutions to do different things. What makes this approach so expensive is the initial acquisition costs, the cost of IT labour to manage the systems on an ongoing basis, software licensing, and maintenance costs.

Very often, companies come to the realisation that their security is no better because it is on-premises. I have yet to see a case of a small to mid-sized company where hosting email in-house is worth it from a cost, security or uptime perspective.

The fact is that IT security is not a core function for most companies. If the internal management of email, web and social media security, as well as other parts of the IT infrastructure, is not a core competency that is central to the success of a business, it doesn't make business sense to keep it in-house. Companies are starting to realise this - and that they can't keep up with the ever-changing threat landscape.

What we are seeing now is a transformation in the way in which IT services are supplied and consumed by companies and individuals. This is true for IT security services as well. The more predictable nature of cloud services costs makes them far more cost effective than deploying and maintaining various on-premises solutions - especially for smaller businesses that take their IT security seriously.

Cloud-based security controls

According to Gartner, more than 30% of security controls deployed to the small or mid-sized business (SMB) segment will be cloud-based this year. We are predicting continued significant growth in all our managed security services this year.

Our Managed Endpoint Security service is also growing as companies recognise the need to refocus on the end point. Security basics like anti-virus and anti-spyware have become such a 'given' that nobody pays attention to them anymore. But effective technologies need to be in place to monitor assets within the IT ecosystem, and protect the information that is stored on them. Especially in light of ransomware which is starting to rear its head locally.

With an effective, centrally managed end point security solution, companies can regain control over the assets in the IT environment more effectively. An effective, properly monitored cloud-based end point security management system gives companies of all sizes the peace of mind that this new blind spot is properly monitored and protected.

While there will always be business cases for on-premises or hybrid solutions, cloud-based, managed services like these are fast becoming the norm.

ABOUT THE AUTHOR

Richard Broeke is IT Security specialist of Securicom