BIZCOMMUNITY

The case for Security as a Service

By Simeon Tassev

25 Oct 2016

Companies have been hard-pressed for many years to look for ways to do more with less, but when it comes to IT, more focus and budget is given to infrastructure, applications, backup and disaster recovery than IT security. This is arguably more critical to core business functions.

Security is considered a costly exercise when multiple technologies are required, along with the resources to implement, manage and monitor these technologies and because such security skills are scarce, attracting and retaining such individuals is challenging.

A company's security also depends on the resources it deploys and their ability to analyse and interpret information proactively in order to prevent threats that could wreak havoc. As a result, the opportunity for human error, in-house management can also be a security system's greatest weakness. Security as a Service (SECaaS), particularly security monitoring and vulnerability management, is a cost-effective, effective solution to these challenges for business IT security.

Ultimately, it's a matter of core competence. Attempting to manage a security task team that is separate from and unrelated to the core of the business is a financial drain and an internal distraction. By partnering with an experienced SECaaS provider it becomes possible for an organisation to focus on what matters most by maximising their resources in the right place.

What is Security as a Service?

SECaaS is a business model whereby security-focused organisations with the expertise and resources provide their technology and human capital to other businesses through integration into their own environment. This is done for the purpose of eliminating the traditional worries that come with capital outlay on technology and the resources required to monitor and manage the solutions to ensure risk is mitigated. Once integration has taken place, the SECaaS provider will put the necessary skilled resources in place to 'man' a Security Operations Centre (SOC) that monitors and manages all security technologies and issues for that business.

This model was designed in response to repetitive challenges plaguing a large number of businesses, when it comes to IT security. With the increasing complexity of IT security, the requirement for specific skills is becoming more obvious, and

the shortage thereof even more so obvious. Attraction and retention of IT security skills is tricky and where security is managed in-house, the situation becomes even more problematic when the separation of duty principle is not adhered to where an individual has multiple conflicting roles. Even though it may not be intentional, the effect is that the individual has the task of executing security policies and policing them, which creates the opportunity for oversight and error. An IT security oversight translates into an open door, which is easy for the wrong person to exploit.

Choosing the right partner

The decision to relieve the business of functions and responsibilities to an outsourced specialist service provider can bring with it many benefits, but must only be undertaken after intelligent evaluation. The key to effective outsourcing is doing so for the right reasons.

When considering security as a service, consider the relationship between the company's operational purpose and the IT security function to be outsourced. Given that IT security is critical to business operation, it's imperative that it be handled correctly and it makes sense to hand this task over to a trustworthy service provider. If an external provider can replicate or improve on the security function under consideration, while cutting costs associated with human resources, employment benefits, training, administration, hardware and the like, then security as a service makes business sense.

The biggest benefit that comes from SECaaS is that expert security service providers have the experience and exposure to different types of organisations and environments. The company on the receiving end of the security service has the benefit of learning from others' mistakes, rather than making their own and learning the hard way.

By partnering with the right security service provider, organisations can rely on security experts to implement the right infrastructure for their needs. Solutions can be deployed faster, with less effort than with on-premises management and skilled external individuals can manage service availability and health monitoring. Software upgrades and security patches are no longer a worry, as someone else will take care of this to ensure effective protection.

Furthermore, security capacity and functionality can be upgraded or changed in response to shifting business needs. Security information and event management tools provided by SECaaS partners are completely customisable when it comes to rule tuning, reporting and dashboards. Therefore, businesses will have overview of the security function, even though it is no longer managed directly in-house.

In short, any organisation that has a serious need for IT security is more than likely to benefit hugely from contracting out. Purely for the reason that a specialist security company's skills, knowledge, and workforce management abilities are dedicated to perform a service so that other companies can focus on their core competencies instead of security.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021

- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...