BIZCOMMUNITY

Is your cloud-based app secure or is it costing you money?

It seems as though each day brings another article about IoT, big data analytics and cloud architectures talking about the unlimited potential for companies trying to gain a competitive edge in an increasingly digital world.

Source: pixabay.com

Early adopters, who are a bit further along the road to digital transformation, are already enjoying some the benefits of the public cloud, like economies of scale, utility billing and more.

“What may not be entirely clear, however, is how the shared security model of the public cloud affects your security responsibilities,” says Simon McCullough, major channel account manager at F5 in South Africa.

“While cloud providers typically do an excellent job of managing the security of their physical data centres, infrastructure and rented systems, they can’t do much about the things businesses deploy or put in the cloud, namely applications, services and data.”

Poor security practices in the cloud
Lori MacVittie 12 Apr 2019

At the same time, according to F5 Labs research, 53% of data breaches initially target the application layer, so, no matter how you look at it, security in the cloud is as important as security in traditional data centres.

Speak to any business owner who’s felt the effect of a breach and you’ll be told that a robust and agile web application firewall (WAF) isn’t a “might do” any more but is rather a non-negotiable.

Traditionally, says another F5 white paper, WAFs were deployed as hardware appliances on premises in enterprise data centres. With applications migrating to cloud-based Infrastructure-as-a-Service (IaaS) environments and organisations leveraging cloud Software-as-a-Service (SaaS) apps, security teams are challenged to protect applications beyond the data centre - without compromising performance, scalability, and manageability.

Enter the WAF

“In our report, titled The Hidden ROI of Cloud-Friendly Security, we talk about the fact that 40% of all traffic can be unwanted bots, malware, scanners and the like and that you, as a business, are paying their way,” he continues.

“Most businesses are billed on a utility basis when it comes to traffic for applications in the cloud and incurs real, quantifiable costs every time a bot makes a request of any resource associated with your cloud account. This means companies are likely paying hefty bills as a result of non-customer traffic.”

Deploying solid security tools, like Application Delivery Controllers (ADCs) and WAFs in front of cloud-based apps can protect these applications and save money by filtering out costly, unwanted traffic while effectively reducing the resources allocated to servicing bots and scanners.

“Using an ADC or WAF in the cloud can deliver a measurable return on the cost of your investment while ensuring services stay available and secure,” says McCullough.

Security tool choice matters to the cloud

Anton Jacobsz, managing director at Networks Unlimited Africa, says it doesn’t end there. “Good security tools can better enable and inform business intelligence,” he says.

The rise of multi-cloud brings challenges and benefits

3 Dec 2018

“A WAF or ADC can make it easier to analyse traffic patterns and data to and from the cloud-based web applications and, with that data at hand, businesses will be better equipped to make resource management decisions that can cut costs quite dramatically.”

According to the 2017 WhiteHat Security Application Security Report, almost all apps contain three or more vulnerabilities, with half of those being critical. This equates to an increased risk of data loss, theft or denial of service if not remedied quite quickly – which is where WAFs can help.

Development teams are now able to use the capabilities inherent to WAFs to address OWASP Top 10 risk areas, mitigating layer 7 DOS attacks, detecting and managing bot activity and foiling zero-day attacks.

“This is all outside of, and without interruption to, normal development cycles,” says Jacobsz. “Behavioural analysis can also prove to be very effective in identifying patterns and managing traffic to and from your cloud-based web applications.

“And, while these capabilities can be difficult to build and manage on your own, a solid security solution provider will help make the implementation of these services simple and effective.”

Jacobsz says boosting security in the cloud is only going to become more critical as time goes by and Cyber Security Ventures’ Cybercrime Report 2016 predicted cybercrime could cost business six trillion dollars annually by 2021.

“You may not suspect anyone of targeting your business but those of a trusting nature are a cyber criminal’s dream,” he says. “The safest approach is to implement security tools that can not only help reduce costs but can also provide the right level of protection for the smooth operation and success of cloud-based applications,” he concludes.