Cloud security

Collected by Abdullah Alaidrous

13 September 2019

Introduction

1- Cloud Security Defined

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

2- Why is Cloud Security Important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

Cloud security offers many benefits, including:

Centralized security:

The enterprise environment has changed drastically over the past couple of years, with organizations relying on both physical and virtual environments deployed either in private or public clouds to improve service availability or boost business capabilities.

The diversity of tools and software that makes all this possible also comes with some disadvantages, one of them involving security and how to manage all these environments as efficiently and cost effectively as possible. Architectural issues such as how to secure virtual

machines that share the same stack of physical resources (e.g. CPU, memory, storage) without affecting their performance have been regarded as difficult – if not impossible – to solve.

Reduced costs: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

Reduced Administration: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

Reliability: offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

3- Cloud Computing Security, Reliability And Availability

Cloud Computing is a technology in which different users are able to access computing facilities from a single multi-provider who normally has the requisite infrastructure and or software and vends them out for a fee. The technology has evolved over the years as a hybrid of different technologies that are looped together to provide services such as Software as a Service (Saas), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Individuals, academics and enterprises choose the services best suited to them and purchase them in an as-needed basis, which forms the attractiveness of Cloud Computing. Issues arising out of cloud computing are similar to those experienced by any other internet based provider, which are security, reliability and availability. With the ever-increasing use of Cloud Computing by enterprises to conduct business activities, these pertinent issues are more important than ever.

Saas, Iaas and Paas

3.1 Software as a Service (Saas)

These types of providers offer applications hosted on the network that lets customers enjoy the software they most require without having to buy them. This allows users to use software they need to use on an as-needed basis, saving on costs if they were to purchase the software themselves. Users are able to avoid paying license fees or additional equipment to operate the software and instead pay fees to the provider for limited access.

The main security concern for users of SaaS is denial of service attacks that may be made towards them directly, or that might affect them when their provider it attacked. In denial of service attacks malware may be injected into the servers that generate useless traffic to the server that slows down access of service by genuine users. Another way that is done is by hackers

giving multiple commands to servers that slow it down and make it hard for other users to be able to enjoy the service sufficiently.

3.2 Platform as a Service (PaaS)

Users who just need to utilize applications that are more capable than what they have presently can contact cloud computing providers of the PaaS caliber to remotely access application, either independently or still using the provider's machines, and without having to install the applications themselves. Also suitable for short periods of use or intermittent use, where purchase would lead to underutilization, or when there is need to use more capable applications than the user has, and they require more capacity.

Users should however be advised that PaaS has some underlying security concerns associated with it, which emerge mostly from the activities of the provider such as third-party relationships they may have with other providers. Combinations of these elements from numerous sources create mash-ups, whose security is suspect, and which also brings the security concerns into the entire platform.

Another security issue with PaaS is the requisite frequent upgrading of features contained in the platform. As the providers strive to keep up with the upgrading requirements of features, applications may get developed too quickly to give sufficient time to seal all security loops and bugs in them. Once the applications have been integrated into the platform, the whole platform becomes susceptible to the bugs.

3.3 Infrastructure as a Service (IaaS)

For organizations that require operational support from the ground up, there is the option of outsourcing every aspect of computing infrastructure such as storage, hardware, servers and other networking components. This allows them to concentrate on other business processes without being overly concerned with their infrastructural capabilities.

IaaS providers make storage facilities, servers, networks and other computing resources available to their users by creating virtualized systems. The security concerns experienced by IaaS therefore come from the virtualization feature of their services such as the hypervisor, which oversees the performance of all virtual machines. The hypervisor therefore becomes a very crucial component of the IaaS that must be secured, as its breach is passed on to the whole system.

4- References

1- https://en.wikipedia.org/wiki/Cloud_computing_security
2- https://speedypaper.com/essays/101-cloud-computing-security-reliability-and-availability
3- https://businessinsights.bitdefender.com/centralized-security-management
4- https://www.forcepoint.com/cyber-edu/cloud-security