Watch and learn

Editorial Type: Feature **Date**: 09-2019 Views: 19 **[More Tags]**

Securing the cloud based on continuous testing and real-time monitoring is an essential cloud security strategy. Aleksander Gorkowienko, Managing Consultant at Spirent SecurityLabs makes the case

The cloud offers organisations some considerable benefits, especially in terms of scalability, cost, and flexible workforce practices, but it also poses its own security challenges. While some challenges are familiar, others are cloud specific and they will require the proper application of current techniques and technology in this brand-new environment.

DEFENCE IN DEPTH

Securing and defending every layer of the business system is a well-established practice in modern IT centred business. Every element of the stack is identified and secured individually, ranging from application access, the network, and hardware levels.

Cloud infrastructure requires the same in-depth defence at every level. However, securing each level can be a challenge, because the security team may be unfamiliar with the cloud environment. Also, some elements of the stack may be difficult or impossible to access.

One of the most significant threats to any infrastructure is still associated with social engineering attacks. These forms of attack are increasing and becoming more sophisticated and highly targeted. In this regard, cloud-based systems are as vulnerable as any other, so defeating the social engineering threat is an important challenge - and while good employee awareness is important, technology based solutions can really help. The effective management of security policies in the cloud is imperative.

Organisations need to create rigorous identity management policies, including two-factor authentication, and enforce them across every part of the cloud. Additionally, email filters must be enforced, updated constantly, and tested continuously against the latest phishing attacks, based on real-time threat intelligence.

SECURE DIGITAL TRANSFORMATION

Organisations are frequently using cloud platforms to deliver part or their entire digital transformation program. This can include capturing, processing and

integrating data from SCADA, ICS, and IoT devices. It also means integrating edge systems into the infrastructure.

Many of these systems are highly constrained, located remotely, and vulnerable to a range of exploits. They expand the attack surface and make securing the cloud environment much more complex and challenging.

Cloud infrastructure is increasingly moving towards software-defined networking (SDN) and its advantages need to be balanced because SDN offers significant benefits for performance and elasticity. It can also make it easier for the cloud infrastructure to respond to new threats or implement updated security controls, often with just one click.

However, SDN introduces potential security pitfalls. Changes in network configurations and functions can be promulgated rapidly throughout an entire infrastructure. Operator errors are propagated immediately, and probing botnets can identify and exploit such errors before the organisation is aware. The recommended defence is continuous adaptive testing of the cloud infrastructure while SDN configurations are being modified.

SECURING THE DYNAMIC MULTI-CLOUD

The cloud has made it easy for different parts of organisations to spin up their own instances within the same cloud host and adopt different cloud providers and infrastructures.

Multi-cloud environments introduce significant security challenges. The threat landscape expands, and managing security becomes significantly more complex. Security policies that work in one cloud environment may not in another. Building effective security across multiple, heterogeneous cloud environments requires a complex setup, supported by continuous monitoring.

The modern cloud is a complex, dynamic environment and it can often present a broad attack surface. Business cloud environments are becoming more heterogeneous. They encompass multi-cloud environments, data input from vulnerable and remote OT and IoT devices and resources that are distributed to edge systems.

Securing such a dynamic, diffuse, and fast-evolving architecture is a challenging task. It requires continuous, comprehensive testing of the platform, based on real-time threat intelligence. Testing must include every layer of the cloud infrastructure, which, in addition, can help to uncover potential vulnerabilities across the digital landscape of the entire enterprise. NC

Email The Editor! OR Forward Article Go Top

PREVIOUS NEXT

Print Article