Why ‘castle-and-moat’ protection is no fairy tale

Our changing world, with its more distributed infrastructure and new applications and workloads exposing a larger attack surface, means that perimeter security, while still an important element within an enterprise's cybersecurity arsenal, is simply no longer enough.

This traditional 'castle-and-moat' principle, which assumes that all security threats come from outside an organisation, has become increasingly problematic. Consequently, many organisations are shifting their focus away from perimeter-based firewalls, and looking instead at the protection of their application workloads, wherever they may reside.

Protecting the changing landscape

The combination of evolving app development and infrastructure that is now distributed on-premises and across multiple clouds – both public and private – calls for a more flexible approach to security. Add to this the fact that the threat environment is on the up, with skyrocketing numbers of increasingly sophisticated threats, and it is clear that identities, endpoints and workloads can no longer be trusted based just on the fact that they are internal to an organisation.

The time to extend perimeter protection to the workload level is now, and importantly, it starts with embracing the Zero Trust model.

A phrase first coined by former Forrester Research analyst, John Kindervag, in the paper entitled, 'Build Security Into Your Network's DNA: The Zero Trust Network Architecture', Kindervag described the concept of Zero Trust as having a straightforward philosophy at its core, saying that 'Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. And so, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

Simply put, Zero Trust allows for the visibility and security controls needed to secure,

manage and monitor every user, device, application and network. Within this model, no traffic may be trusted – unless policy proves otherwise.

The Zero Trust approach calls for the monitoring and protection of east-west traffic also, described as the flow of traffic within a datacentre, which has increased as a result of the adoption of converged and hyperconverged infrastructure, virtualisation and the private cloud.

Micro-segmentation: controlling who accesses what

A key part of the Zero Trust philosophy is micro-segmentation. Here, workloads are isolated from one another and individually secured, improving control of lateral east-west traffic within the datacentre. This is of particular importance with the recent growth in remote working, as micro-segmentation must cover all users – regardless of location – as well as all of a company's resources, be they on the cloud or within the datacentre.

Reducing lateral movement is not the only benefit of workload protection. It also facilitates the identification of workload behaviour deviations due to the faster detection of malware execution patterns, exposes vulnerabilities within software packages and promotes compliance. This includes compliance not only to the applicable laws and mandates, for example the Payment Card Industry Data Security Standard (PCI DSS) and the Protection of Personal Information (POPI) Act, but also to internal company rules and regulations.

Creating consistent, layered security

The adoption of a Zero Trust policy means that companies are able to approach security-related challenges in a new way. By ensuring the security moves everywhere the workload does, it provides a consistent, layered security approach right across the multi-cloud environment, allowing for improved visibility and automation, reduced risk, and a reduced attack surface.

Hardus Dippenaar, Senior Network Architect at Datacentrix

> Simply put, Zero Trust allows for the visibility and security controls needed to secure, manage and monitor every user, device, application and network. Within this model, no traffic may be trusted – unless policy proves otherwise.

For more information on please contact Elzette du Preez on edupreez@datacentrix.co.za

www.datacentrix.co.za