Zero Trust cybersecurity approach vital for besieged local businesses

By Andre Lombaard
Technical Manager: Security at Datacentrix

At the end of 2021 a report released by the International Criminal Police Organisation (INTERPOL) painted a fairly bleak picture of the cyberthreat landscape in South Africa.

Entitled the *African Cyberthreat Assessment Report 2021*, the survey highlighted that, while the broader African continent had experienced some attacks against critical infrastructure and frontline services, South Africa was amongst the countries hardest hit, experiencing around 230 million threat detections in total between January 2020 and February 2021. Comparatively, Kenya and Morocco were subjected to a much lower number of attacks, at 72 million and 71 million respectively over the same period.

In South Africa, 219 million detections were related to e-mail threats, and the country was also listed as the most targeted with ransomware and Business Email Compromise (BEC) attempts. In fact, the INTERPOL report referred to figures from Accenture, which stated that South Africa has the third highest number of cybercrime victims worldwide, at a cost of R2.2 billion a year.

“

The INTERPOL report referred to figures from Accenture, which stated that South Africa has the third highest number of cybercrime victims worldwide, at a cost of R2.2 billion a year.

It is clear that local business needs to reconsider its cybersecurity approach, and that the pre-COVID Virtual Private network (VPN) setup that permits users to access all areas of the network, is no longer a secure strategy.

In fact, today's world of remote working and cloud-based systems necessitates a 'Zero Trust' approach to keep a business' data and infrastructure secure. This type of strategy, based on the premise of 'never trust, always verify', revokes any type of access privileges that users may have previously had on a network,

> A Zero Trust approach to cybersecurity can essentially assist any business to create a safer remote and cloud environment, simplifying the security architecture and reducing organisational risk.

and keeps their access to the absolute minimum, while frequently requesting user authentication.

Check, check and check again

In a Zero Trust world, legitimate, authorised users may access *only* those areas of the network, as well as apps and data, that are needed to complete a task (for instance an organisation's enterprise resource planning (ERP) software, e-mail, and a document repository) and nothing more.

Here, technologies like Secure Access Service Edge (SASE), in combination with biometrics on end point devices as well as privileged identity management (PIM) solutions are playing a critical role in helping companies to scale down access and increase the security of their systems.

These technologies allow for the security perimeter to be moved away from the enterprise to the user or device. They then require users to be regularly identified and verified, before permitting them to enter the network perimeter, and provide only pre-assigned access to certain areas.

Policy management critical

Designing a Zero Trust architecture must include, at its core, centralised policy management, which encompasses identity-related and allocation policies. It must also align with local governance requirements,

Andre Lombaard, Technical Manager: Security at Datacentrix

such as The Payment Card Industry Data Security Standard (PCI DSS), the International Organization for Standardization (ISO) or General Data Protection Regulation (GDPR), regarding the safety and security of data and cloud infrastructure.

The alignment of processes and policies is essential, while it might be possible to control the technology, it is not necessarily possible to control the human behind the device; this remains a major anomaly when it comes to cybersecurity. However, while you may not be able to change user behaviour, it is possible to enforce processes and policies to best control engagements – leading to one path and one path only.

A Zero Trust approach to cybersecurity can essentially assist any business to create a safer remote and cloud environment, simplifying the security architecture and reducing organisational risk.