4 trends paving the way for the future of cybersecurity in South Africa

By Colin Erasmus

22 Jun 2023

It was around three and a half decades ago that the world experienced its first major security attack. The Morris Worm shut down 10% of the internet in just 24 hours, sending unsuspecting businesses into a tailspin. And so it was, that the very first Computer Emergency Response Team was born, marking an important milestone in modern cybersecurity.

Colin Erasmus, chief operations officer at Mcrosoft South Africa | image supplied

Looking back, it's fascinating to see how far incident response has come – especially as we stand on the cusp of another tidal shift in the tech landscape. With the revolutionary capabilities of AI in the spotlight, the future of cybersecurity is a key topic of conversation – especially for businesses in South Africa that have proven to be vulnerable to attack.

As a new era in cybersecurity unfolds, these four key trends will help shape the security discourse.

1. Ransomware is becoming more sophisticated

While Africa – and South Africa – have always been a prime target for malware and ransomware attacks, these occurrences are increasing in number and sophistication.

In fact, Interpol's Africa Cyberthreat Assessment report found that South Africa leads the continent in the number of cybersecurity threats identified, and that it also has the highest targeted ransomware and business email compromise (BEC) attempts.

Recent Microsoft-IDC research on Enterprise Security Trends shows that the growing number of ransomware attacks is among the top three security priorities for South African organisations, with 45% identifying protection against harmful ransomware and malware attacks as a key focus area.

Moving forward, hackers will continue to use these tried-and-tested techniques, but will also make use of AI to enhance the speed and accuracy of attacks.

Smarter workplaces provide hackers with new entryways to networks

Over the past few years, South African organisations have made significant changes to their cybersecurity strategies to accommodate the growing number of remote users that need access to mission critical data and applications.

The Microsoft-IDC research reveals that organisations are placing the bulk of their focus on endpoint security and access management solutions, with 65% already invested in endpoint protection solutions and 61% in access management.

But while IT teams have been preoccupied by remote work, largely perceiving ransomware as an IT-focused threat, these attacks have become more prevalent in operational technology (OT) environments – including everything from industrial equipment to HVAC controllers and elevators.

Microsoft's threat intelligence has revealed an increase in threats exploiting OT controllers and IoT devices like routers, printers and cameras, driven largely by hybrid workplaces and the growing interconnectivity among organisations.

The IT world is increasingly being brought together with the OT world, introducing new and severe risks, with attackers now able to jump between formerly physically isolated systems. Suddenly everything from cameras to smart conference rooms are providing hackers with new entryways into workspaces and other IT systems.

AI is becoming more mainstream

The good news, however, is that AI and machine learning are arriving in technology's mainstream. The Microsoft-IDC research shows that around 39% of companies in South Africa plan to address security concerns by improving the automation of processes and integration of technologies.

And while there has long been a perception that attackers – even those using age-old techniques – have the advantage of surprise, AI can swing the agility pendulum back in favour of defenders.

AI empowers defenders to see, classify and contextualise much more information, much faster. Its radical capabilities and speed give defenders the ability to deny attackers their agility advantage.

The growing skills gap will become less challenging

AI also enables human defenders to operate more quickly and efficiently than before. This is key for IT teams across the region, given the growing skills gap among security professionals. Around 53% in South Africa identified upskilling as a

vital step to increase the level of security in their organisation, according to the Microsoft-IDC research.

Automated and intelligent tools empower security professionals to focus on security strategy and culture rather than sitting behind a computer watching and managing incoming signals that indicate attacks or zero-day vulnerabilities. The more teams can use AI to provide clear views of cyberthreats, the more they can open the door for entry-level talent while also freeing highly skilled defenders to focus on bigger challenges.

AI is a new area for defenders, and as organisations increasingly develop new AI systems, they need to understand how these systems can be breached, and how attackers can leverage AI systems to carry out attacks.

Though AI won't be the silver bullet that solves security in 2023, it is the turning point for rapid acceleration in protecting against bad actors. Businesses simply cannot afford to underestimate the way AI innovation over the next few years will impact the security industry in South Africa.

ABOUT THE AUTHOR

Colin Erasmus, chief operations officer (COO) at Microsoft South Africa.