BIZCOMMUNITY

Why Africa is a popular target for cybercriminals

Over the past few years, the African continent has been the target of multiple cyber attacks. This year Dis-Chem saw 3.6 million records exposed in a data breach, while TransUnion was held to a R225m ransom in March. Nigeria experienced financial institution hacks and Kenya experienced a radical increase in financial phishing attacks.

Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa | image supplied

The continent itself is perceived to be the most cyber-attacked on the planet. Added to this pile of concerning numbers are the financial ones that cited Africa losing around $4bn annually to cybercrime.

As Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa, highlights, there are numerous obstacles that have to be overcome to shift this dynamic and make Africa a safer digital place.

“One of the key issues impacting cybersecurity safety on the continent is the lack of regulation,” she adds.

“The problem is that only 29 of Africa’s 54 countries have established national cybersecurity strategies. There has to be a far more coherent effort on the part of government and the public sector to address vulnerabilities and to embed a deeper, continent-wide commitment to security.”

Inside the mind of the attacker: How cybercriminals think when they enter organisations

25 Oct 2022

This slow uptake on the legislative and government side is reflected on the business side as well. While some organisations have implemented rigorous security controls and initiatives, many are still playing fast and loose with the digital rules.

As the Club of Information Security Experts in Africa (Cesia) found, only 52% of companies in Africa believed that they were able to handle a significant cyber attack, and this statistic is compounded by an Interpol report released in 2021 that found more than 90% of companies in Africa did not have adequate cybersecurity protocols in place.

“On top of the lack of legislation that has not caught up with cybercrime, there are other factors at play here,” says Collard.

“One is the lack of user awareness – people are still not getting enough training around the threats or how they are vulnerable to them, or how they introduce these vulnerabilities to the organisation. It has become absolutely essential that there are more user awareness campaigns and training. This can significantly mitigate the likelihood of a successful attack.”

Of course, this ties into another threat that impacts Africa – resources and skills. These are in short supply, which makes it challenging for companies to build up the teams and resources they need to actively address the vulnerabilities and security.

A recent IDC report titled *The Impact of Cyberextortion on Africa* pointed out that IT security teams are struggling to handle the increased exploitation of vulnerabilities both inside the business and within remote working. This fresh dynamic has put increased strain on already stressed systems and security professionals.

“Another reason why Africa has become so popular is the fact that companies have largely leapt on the digital bandwagon, with a significant number of companies planning to increase their connectivity, IoT investments and digital transformation initiatives over the next 12 months,” says Collard. “

This is fantastic for improving operational value, driving growth and so much more, but it also increases the cybercrime attack surface. The number of cyber-attacks made on organisations in Africa have grown alongside the gross domestic product and corporate expansion.”

South African data breach costs reach an all-time high, report finds

28 Jul 2022

Although many companies have taken a firm stand against cybercrime and are implementing cyber strategies, they are playing the catch-up game while the cybercriminals are ferreting about in their systems and taking advantage of unexpected vulnerabilities.

To resolve these challenges, companies and governments alike must invest in training, innovative solutions, skills development and regulations that create security resilience and strength in the face of this threat.

“The sophistication of threats will continue to grow so organisations need to maintain their commitment to investing into cloud security, data and privacy, application security, and emergent technologies such as AI and ML,” concludes Collard.

“These investments coupled with ongoing training and awareness will give companies a fighting chance and a stable security foundation from which to combat the threat.”