BIZCOMMUNITY

SA enterprises can benefit from AI cyber protection

By Steven Kenny

17 Oct 2023

South Africa is leading the way in cybercrime across Africa. In 2022, the country detected a staggering 230 million threats, far outstripping Morocco, which came in second place with 71 million threats. South Africa also bore the brunt of the highest number of targeted ransomware and business email compromise attempts. It ranks third globally for the number of cybercrime victims, with an annual cost of R2.2bn.

Cybercrime has become a lucrative business for threat actors who are utilising innovative tools to carry out their attacks. However, cybersecurity is constantly evolving to meet these threats and cater to the ever-changing needs of individuals and organisations.

Enterprises are not only gaining access to but also beginning to utilise innovative solutions that bolster their security resilience. artificial intelligence (AI) is playing a pivotal role in this process. It can help enterprises secure their growing attack surface area and identify and rectify vulnerabilities without necessitating additional human intervention.

Celebrating Africa's top 5 smart cities: Showcasing progress and prowess

Marcel Bruyns 5 Jun 2023

However, deploying AI-driven solutions is not without its challenges. Enterprises need a robust strategy in place that considers the long-term feasibility and requirements of these solutions as part of any business change.

Threats of escalating severity

For many threat actors, cybercrime is a business like any other. As a result, they are inclined to adopt the latest trends and use the latest technologies to carry out their attacks. The various features of AI and machine learning (ML) that enterprises are starting to explore are the same features criminals are misusing.

There are several examples of this. For instance, generative AI tools such as ChatGPT and Google's recently launched Bard can provide criminals with marketing messages for phishing emails. AI automation tools can be used to create automated interactions with a large pool of potential victims. Algorithms trained on personal data can be used to build profiles of victims and prioritised lists, minimising the resources needed to do so while increasing the accuracy of attacks.

However, the misuse of AI goes beyond straightforward phishing attempts using ChatGPT. AI-powered malware can leverage advanced techniques to evade detection by security software and use metamorphic mechanisms to change operations based on the environment they're in.

Consider DeepLocker, an AI-powered malware developed by IBM research as an experiment. It conceals its intent until it reaches a specific victim, potentially infecting millions of systems without being detected. It is critical that enterprises stay one step ahead of malicious innovation like this, and they can do this by properly integrating AI-powered systems and countermeasures into their security strategies.

First responders

Having AI-enabled security systems requires an overhaul of organisations' inner security workings. In other words, given the technological, legal, and ethical implications of those systems, companies need to provide adequate training and education for their security teams, as well as conduct due diligence with their respective IT suppliers and partners.

From there, the key factor is data. AI programmes can identify patterns, detect anomalies, and analyse vast amounts of data throughout an organisation's network and infrastructure. This applies to infrastructure regardless of its scope and circumstance. Case in point, AI can be used to detect vulnerability in hybrid or remote environments where systems are decentralised.

These programmes serve as the "first responders" in countering any malicious activity, and they help organisations assume a more proactive, forward-looking risk posture.

AI is also a force for reducing organisations' security workloads. For example, AI-powered automated patching can track and patch important software in real time and minimise potential exposure to threat actors. Keep in mind, businesses should not become over-reliant on these systems, or leave them susceptible to data breaches. To avoid this, organisations must implement solid policies and guidelines regarding data access, monitoring, and analytics.

We need to embrace the future

According to Microsoft-IDC research, 39% of companies in South Africa plan to address security concerns by improving the automation of processes and integration of their technologies. This is a step in the right direction, but it is only the beginning for many organisations and their efforts to overhaul their security setups.

AI represents a turning point in how we approach, among many other business functions, security. Its implementation may come with unanticipated consequences, but organisations need to be prepared to adopt it, lest they fall behind their competitors or only see its value too far down the road.

ABOUT THE AUTHOR

Steven Kenny is the EMEA architect and engineering program manager at Axis Communications