The extremely unsecure crystal ball: cybersecurity in 2023

Anna Collard, senior vice president of content strategy and an evangelist at KnowBe4 Africa, shares some 2023 cybersecurity trends.

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

“Looking ahead at 2023, it is very likely that there will be a continued increase in the sophistication and prevalence of mobile malware attacks, particularly against Android devices,” says Collard

“In 2022, the FluBot trojan really did sweep through Android phone users, stealing passwords, online banking details and sensitive information. It was extremely effective, and it is very likely we will see more of this type of attack in 2023.”

Another area of concern lies in the increased use of internet of things (IoT) solutions.

This technology has been lurking in the wings, full of promises about the connected future, for years, but now it is finally finding its digital feet and making inroads across smart cities, organisations and solutions. However, it is also a significant risk.

“Operational environments, such as Scada, are becoming increasingly digitised and more inclusive of IoT technologies,” explains Collard.

“This means that where a malware infection could have potentially only impacted a company’s administrative network in the past, the interconnected and digital transformation of these systems now makes them all open to risk. This can impact a company’s downtime, but it can also impact the physical safety and well-being of employees. Even worse, we have noticed a shift amongst threat actors away from financial services to the manufacturing industry”

This situation can evolve within high-risk plants or manufacturing environments where systems are digitised and connected to enhance worker or machinery safety. If these systems are hacked, it could lead to unexpected problems or safety issues. If there is not the right amount of security in place, then the increased attack surface presented by digitised systems creates more opportunities for cybercriminals.

“Of course, the more complex systems get, the more difficult it becomes to properly secure them,” says Collard. “There is IoT and there is operational technology, and then there are interconnected cyber-physical worlds or systems such as autonomous cars and digital twins that increase the attack surface. The keyword for 2023 is vigilance. Companies need to become more vigilant, and they need to be more prepared for what lies ahead.”

More investment in security

On the other side of the cybersecurity coin, however, is the fact that decision-makers across all levels of the organisation have become more aware of security, and more invested in implementing it properly. This trend sharply rose in 2022 and will continue on its upward trajectory well into 2023 – and this will go a long way towards helping companies be better prepared for the onslaught that lies ahead.

“Board members and decision-makers are putting security and resilience on the agenda,” says Collard.

“They are aware that cybersecurity is a growing problem, and this is being driven by the media and by changing data privacy and protection laws, as well as by a more people-centric approach to business. Companies are recognising the importance of security protocols for protecting their employees and their data, and putting the right processes in place.”

Looking ahead, it is hard to predict precisely what vector, threat, attack surface or vulnerability will be exploited by cybercriminals in 2023. What is easy to predict is that they will try, and keep on trying, because it is a business, and a profitable one. To combat the risks and embed a culture of security within the business, companies need to focus on training, security skills development, robust security solutions, and constant awareness.