FIT FOR A SECURE FUTURE – WHY CYBERSECURITY IS ABOUT MORE THAN STAYING SAFE

To safely accelerate your business operations and embrace new technologies, it's crucial that your organisation has robust cybersecurity measures in place.

Kabelo Makwane – Managing Executive: Cloud, Hosting & Security at Vodacom Business

Kabelo Makwane, Managing Executive: Cloud, Hosting and Security at Vodacom Business, believes that to be fit for the future, businesses need to take a proactive approach, planning ahead to ensure that security is a seamless part of their journey.

"We are putting more emphasis on the human behaviour aspects of cybersecurity," Makwane says. "One of the best ways of improving your security resilience is by changing the behaviour of your people. A lack of cybersecurity awareness can be the weakest link, and, in some cases, this aligns with the engineered aspect of threats. It's essential to create a culture of cybersecurity awareness and constantly reinforce security priorities."

Cybersecurity parameters have changed as the nature of work has transformed. Today, "work from home" might not mean working from an actual dwelling, but from wherever an employee happens to be based. Enabling this flexibility is becoming increasingly important for employers. Not only does it allow for differently abled workers, such as wheelchair users, to work in greater comfort and safety, but it also appeals to the Generation Z and Millennial talent pool, who are making workplace flexibility a prerequisite for accepting a job.

"These days, organisations need to offer the opportunity for employees to integrate work and home seamlessly, but it brings a lot of cybersecurity challenges and the guardrails must be clearly defined. For example, using public WiFi for work activities should be disallowed, as this can open up massive threats and vulnerabilities," Makwane says.

Furthermore, the option for employees to use their own devices requires governance. Cybersecurity policies must apply to all devices.

"Policies like banning the use of USB devices and rather using trusted, shared storage mediums can improve security. This also fosters a collaborative culture, while giving people the agility they require to do their job remotely," Makwane adds.

HYBRID WORKSPACE

Providing the freedom for people to achieve their work-life balance can boost productivity greatly – but with this freedom comes the need for greater responsibility in many aspects.

Tools to measure productivity – to ensure that employees are reaching their productivity goals during their workday, but are still able to switch off after hours – are essential. Says Makwane: "Analytics are important in helping people manage their time effectively. Implementing boundaries and focusing on the mental health of employees are important aspects of embracing the transformation of the workplace."

Another aspect is the management of the office space. In a hybrid workspace, IoT-enabled technology can facilitate a smarter working environment. Energy efficiency in unused areas can optimise the environment in terms of air-conditioning and lighting. Facility management can help reduce costs. For example, the amount of real estate could be downsized to fit the actual use.

And, of course, one of the biggest focus areas in a hybrid work environment is security. "A lot of cyber-attacks (or ransomware attacks) and incidents go unreported because if they became known in the public domain, they would have a severe reputational impact on the organisations affected. This means that there are likely more incidents and breaches than what gets reported publicly," Makwane warns. "The evolution of cyber threats is creating huge challenges for businesses.

> "At Vodacom Business, we are able to give organisations the opportunities to focus on what will help move them forward, rather than them spending time and resources on keeping their environment secure. "

Threat actors are not standing still, they are evolving. Enterprises need to employ holistic approaches to cyber defence, which includes machine learning, analytics and artificial intelligence for threat intelligence-gathering and behavioural monitoring, a task that would be very complex and time-intensive for humans to accomplish manually."

SECURITY CULTURE

Vodacom Business offers a customisable securitycyber management service to assist with every organisation's needs. This solution can be tailored to small and medium-sized enterprises, and large multinationals alike.

The solution deploys the best-of-breed technologies and integrates them with expert services and highly skilled professionals who ensure they are fit for purpose for each entity.

"The most important advice for larger organisations is to establish a security culture, and this starts with your people, followed by the deployment of a multi-layered security infrastructure. Regularly doing a benchmark in posture assessment because threats evolve fast, and assessing your maturity on an ongoing basis should form part of standard practices," Makwane says.

The challenge for SMEs is that small business owners often have to be the equivalent of a Swiss army knife – they keep the business running end-to-end. "To layer these responsibilities with the specialised ability to be a CIO can be onerous," Makwane says. "Vodacom Business is able to alleviate that burden by offering the deployment and management of security and threat mitigation, in a very affordable, adaptable way.

"At Vodacom Business, we are able to give organisations the opportunities to focus on what will help move them forward, rather than them spending time and resources on keeping their environment secure. We are well positioned with our capabilities to do this at scale. Our end-to-end services are based on our own business experiences, which enables us to understand key business needs and assist small and large businesses alike," Makwane says. ■

Web : www.vodacombusiness.co.za

vodacom business