Soft target - healthcare industry must prepare for the next wave of cyberattacks

While healthcare providers must accelerate their digital health maturity as it directly improves operational efficiencies, quality of patient care and improves protection of personal and sensitive information, it also provides a greater platform and risk for cyberattacks.

123rf.com

While healthcare is a booming industry, it is fraught with strict regulations and high revenues, that provide an environment for cybercriminals to target every aspect of its operations, especially where technology is optimally utilised.

“Due to regulations related to the Protection of Personal Information (PoPI) Act, the need to use, manage and store sensitive patient data creates an increased risk of falling victim to cybercrime. This is further exacerbated by electronic medium of payments for healthcare and the interconnectivity of public and private service providers,” says Shiraaz Joosub, healthcare sales executive at T-Systems South Africa.

There are two main motivators for attacks on healthcare facilities. “The first is the treasure trove of valuable data in the form of healthcare records that contains confidential and sensitive personally identifiable data and often includes credit card or other banking-related information.

The second rests on the fact that healthcare organisations cannot afford disruption to their patient care systems, making the industry a prime target for ransomware and similar attacks. Criminals depend on the fact that payment will be forthcoming to avoid potential loss of life," says Lukas van der Merwe, security sales executive at T-Systems South Africa.

Easy to breach

In addition, the prevalence of internet of things (IoT) devices in healthcare intuitions, as well as the use of outdated healthcare appliances, coupled with a workforce that prioritises patient care over cyber security, means it is often relatively easy to breach a healthcare institution.

Joosub points out that cyberattacks in the healthcare industry could be very crippling and impact business operations, leading to significant downtime, as well as putting staff and patients at risk. “Apart from the obvious implications of a data breach, the most concerning impact of a cyberattack on a healthcare provider is disruption to patient care. In a worst-case scenario, this is life threatening to those patients affected. Criminals often attack in the wake of disaster, when patient care is vitally important, and the number of attacks during the pandemic is testament to that.”

Van der Merwe says that like any other industry, in healthcare the focus has been on protective measures related to the IT systems deployed. Yet much more focus should be placed on a holistic assessment of the attack surface and measures to prevent an attack or breach. “This includes focus on increasing the cyber security awareness of all practitioners, which remains one of the weakest links and last lines of defence. There should also be more visibility of the environment through proactive monitoring and the adoption of next-generation cognitive technology to facilitate rapid response to any anomalous activities observed.”

Significant value

Joosub adds that crisis or incident response plans are generally executed reactively to an event and are not a preventative measure. They do, however, add significant value if these plans are robust and practiced ensuring rapid response to limit the extent and impact of a breach when it takes place.

At the same time, Van der Merwe says, simulation plans are generally not linked to specific technology, but rather define how an organisation responds to events. It is critically important to ensure a robust plan includes a clear understanding of the organisation’s attack surface, the specific risks and the actions required in response to each of the risks identified.

“In addition, such a plan should span all levels and functions and not only the technical recovery. A holistic robust plan will include how the organisation communicates with its stakeholders and how each potential risk may impact on the operational capability of the organisation to ensure alternative potentially analogue alternatives are leveraged,” he says.

Van der Merwe adds that it is important for the healthcare industry to adapt to an ever-changing cyberthreat landscape. “Change is not easy; however, it is a necessary component of a strong defence. By making sure that you are following current security best practices and are aware of new trends in the security landscape, you can be better prepared as threats continue to evolve.”