Now is the time for a full-service cyber security solution

Apart from the obvious risk of contracting coronavirus and getting seriously ill during this worldwide pandemic, there is also a greater risk for companies' ICT systems to get infected by viruses and experience increased attacks by cybercriminals, says Pieter van Zyl, CTO at Reflex Solutions.

Pieter van Zyl, CTO at Reflex Solutions.

“There has been a drastic increase in cybersecurity threats as a direct response to the Covid-19 pandemic and the lockdown regulations to stave off the spread of the virus. As employees were forced to work from home, companies had to open their systems to accommodate this. It created a new market for cybercriminals to exploit. A great number of organisations, without thinking, simply unlocked access to their systems trusting the security of their employees working off-site, without even the typical network operating system (NOS) firewall capabilities.”

“Companies must use a secure Virtual Private Network (VPN) connections to allow remote workers to access the network safely. Secure VPNs allows for enterprise-level security capabilities at home. Consumer-type firewall protection is not enough and home-users’ IT security is not sufficient to effectively defend an organisation against cyber-attacks,” explains van Zyl.

Trend Micro reported that nearly one million spam messages have linked to Covid-19 since January 2020 and the World Health Organisation (WHO) states that there has been a five-time increase in cyber attacks focussed on the increase in funding initiatives created by the pandemic, during April this year in comparison to the same time last year (2019). The rise in monetary gains through these funding initiatives is a drawcard for cybercriminals.

“We have seen an increase in attacks for financial gain during this time of Covid-19, fuelled by the opportunities presented by the increased number of funding actions. It is not only consumers and small businesses, in desperate need of money to survive during this time, but the larger organisations, offering the funding as well as banks are targets too,” says van Zyl.

ZDNet has reported that there has been an unprecedented 238% increase of cyber-attacks against banks specifically due to Covid-19.

There are various cybersecurity threats cybercriminals use to gain personal information or company data. Threats are becoming more complex with enhanced malware: computer viruses, spyware, and worms. Phishing attacks are more believable and it’s easier to be scammed. Ransomware attacks, like the City of Johannesburg and the City Power attacks late last year, block systems and threaten to leak personal information over the internet if not paid a sum of money have become daily occurrences in the business world.

To best secure your organisation not only during this time of the coronavirus but in general, you need an end-to-end security solution that is active 24/7/365.

“Our recently launched Security Operations Centre (SOC) can protect your business from cyber threats through a multi-layered approach. It offers a full-service cybersecurity consultancy where we take over the day-to-day tasks of securing and managing your network while you focus on your core business,” he says.

Training enterprises and their staff to effectively manage security risks, which van Zyl notes is key to secure a business, is part of the SOC offering. “Protection starts with people. All employees should receive awareness training about all the possible backdoors to the organisation’s system. For instance, employees working from home do not realise that their online home security system and CCTV cameras can be hacked and used to gain access to their employer's network when they log on to the system. Teaching users to spot clever phishing attacks is another area individuals should be educated about to guard against being deceived,” van Zyl concludes.

Enterprises need to guard themselves and their employees against security threats of all kinds and one of the ways to do so is to implement a full-service cybersecurity solution, which will assist in mitigating any security risks. The SOC will reduce security risks across the entire connected environment of an enterprise through four key services consisting of: Managed Security Services, Security Assessments, Security Design and Security Compliance.