datacentrix

Phishing, ransomware on the rise in SA due to lockdown

People are currently most susceptible to cyberattacks, given not only the higher number of remote workers than ever before due to the COVID-19 pandemic (which brings its own complications), but also their heightened emotional vulnerability during these difficult times. So says Ahmed Mahomed, CEO at Datacentrix.

A recent report by independent global business advisory firm, FTI Consulting Inc., revealed that local businesses were already under immense security pressure due to a 'lack of cybersecurity preparedness, which continues to create problems and risks for companies in South Africa'. The 2020 FTI Consulting Resilience Barometer also stated that, 'while most leaders in the region are aware of the risks – 84 percent surveyed believe they have cybersecurity gaps – less than half said they have made investments in that part of their business in the last 12 months. This disparity between known risk and response is concerning even during the best of times.'

It continued: 'Recent changes in the ways we are working have presented cybercriminals with a multitude of opportunities to exploit weaknesses in systems, processes, and behaviour. In addition to simple email phishing scams, employees are expecting non-standard emails from their IT support teams, making them more susceptible to work-related phishing attempts.'

Mahomed explains, “We're currently seeing more scammers than ever before preying on people to gain access to sensitive information for nefarious purposes. Unfortunately, the organisational chaos that ensued out of necessity to keep businesses up-and-running following President Cyril Ramaphosa's initial lockdown announcement at the end of March, exposed unexpected technical vulnerabilities that were of great advantage to cyber attackers. Staff are no longer protected behind a corporate firewall, making it more difficult to manage who is accessing what information, when.

> “The best place to start is to complete a cyber posture assessment, which evaluates the current security posture – from security patch management, machines without security solutions, the use of public Wi-Fi, uploads, password age policies and the like.”

“Add to this the fact that we're receiving countless phishing mails masquerading as urgent lockdown-related announcements from schools, the

Department of Basic Education, or health organisations among others is the order of the day. The intent is to use our insecurities, confusion and emotional responses against us to gain access to sensitive information.

“Furthermore, with the growing use of IoT devices, the corporate attack surface has changed for good. We're no longer just protecting corporate brick and mortar; the breaching of vital equipment that can be ransomed for digital currency is a very real and current threat.”

So, how do local businesses go about protecting not just physical corporate assets, but more importantly, the valuable data residing on these devices?

“We must be more vigilant than ever before, that much is clear, and the protection of your data elements translates to cybersecurity right through to the edge, encompassing mobile device protection, a mail scrubbing engine and more. The best place to start is to complete a cyber posture assessment, which evaluates the current security posture – from security patch management, machines without security solutions, the use of public Wi-Fi, uploads, password age policies and the like.”

By measuring an organisation's 'attack surface', which describes a total sum of the vulnerabilities and weak spots in a network or environment that are accessible to a threat actor or can aid the threat actor with malicious intentions (such as committing data theft and compromising assets), it is then possible to identify best practices and highlight parts of the environment that are particularly vulnerable and may require attention.

“A very important point to remember is that people operating within a more relaxed home environment are naturally less vigilant, so companies must also incorporate regular user awareness training, taking decisive steps towards ensuring that employees are continuously educated on how to manage corporate assets outside of the work environment.”

Ahmed Mahomed, Datacentrix CEO

“Furthermore, with the growing use of IoT devices, the corporate attack surface has changed for good. We're no longer just protecting corporate brick and mortar; the breaching of vital equipment that can be ransomed for digital currency is a very real and current threat.”

For more information on Datacentrix' cybersecurity services, please visit https://www.datacentrix.co.za/security.html

www.datacentrix.co.za