BIZCOMMUNITY

It's time to get cyber security basics in place

By Simeon Tassev

23 Aug 2016

Everything in our digitally-connected world has the potential to be infiltrated and exploited by cyber criminals. Levels of online fraud, digital crime and corporate espionage are rising steadily, while legislative steps are not being taken quickly enough in response to provide tools with which to combat cybercrime.

This exponential growth means that cybercrimes can be perpetrated against those who are without adequate legal recourse. As a result, organisations and individuals need to be vigilant in their own right, and take action to defend against malicious cyber-attacks by ensuring that they have a minimum level of security in place, at the very least.

SA cybercrime legislation still pending

The biggest challenge in cyber law is the fact that cybercrimes have not yet been defined and legislated as crimes under which individuals can be prosecuted. Even if an individual is caught with hacking software in the process of hacking an organisation's system and is arrested, there is currently no law under which that individual can be prosecuted.

So authorities either have to release the individual or prosecute him for another crime, like theft if it can be shown that the individual made a personal gain through his actions. Given the scale of possible crimes that can be committed in cyberspace, this is not ideal. The Cyber Crimes Bill of 2015, though still currently tied up in the participatory phases of the South African legislative process, aims to eliminate the challenge. Once passed into legislation, it will be possible to enforce laws specific to cybercrime through prosecution.

Take protection into your own hands

While legislation still has some catching up to do in terms of cybercrime, it's still up to us to defend ourselves against falling victim to cybercriminals. Within cyber protection, the bare minimum in today's digital environment is perimeter protection and endpoint protection. Although these two security measures complement one another, having one doesn't eliminate the need for the other.

Under perimeter protection we see things like intrusion provision, as well as the ability to securely analyse traffic, which takes care of external connectivity and possible threats from the outside. Should perimeter protection fail, endpoint

protection is the last line of defence, regardless of what the endpoint device may be. Once the basic foundation is in place with these two measures, it’s possible to focus on various controls and protection layers, until the business protection objectives have been met.

Commit to the right specialist

Security and cybercrime consultants can be critical in finding efficient solutions for your business. The title 'specialist' is key and the right specialist can assist you in choosing your strategy and will make sure it’s in line with your business requirements. Protection against cybercrime also needs to account for disaster recovery and have contingency plans for different aspects of unavailability of systems or data, and must take into consideration cybercrime trends when strategising.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...