Publication: Sowetan
Page: 9
Title: Prevention is still better than cure as cybercrime rises
Publish Date: 20 May 2020
AVE: 62504.4
Author: Simeon Tassev

Prevention is still better than cure as cybercrime rises

By **Simeon Tassev**

In terms of risk versus reward, cybercrime is a highly lucrative industry. Research from Atlas VPN suggests that cyberattacks generate more than $1.5 trillion (R27 trillion) in revenue each year, and this figure is growing.

This indicates that incidents of cybercrime are on the increase globally, and SA is no exception.

In fact, SA has become a very attractive target, and the damage done by cyberattacks is beginning to add up.

We need to shift our focus from reacting to attacks when they happen, to actively working to prevent them.

The South African technology landscape is an interesting dichotomy that makes it vulnerable to attack by cybercriminals.

On one hand, the market is mature enough that many large international organisations have a local presence, so there are many lucrative potential targets for attack.

On the other hand, our technology landscape and skills base is not mature enough to protect against all of the possible threats and vulnerabilities.

According to IBM Cost of a Data Breach Report 2019, the average cost of a data breach in SA is at R36.5m, which ranks us at number seven of 16 countries.

The reality is that this is not a new scenario, but the frequency of incidents is on the increase and the high profile nature of attacks is growing.

In 2019, we saw several prominent ransomware attacks on local government and utility providers, and the attacks continue even this year, with a recent attack on vehicle recovery organisation Tracker.

Aside from the disruption to service that successful breaches cause, there are numerous other ramifications that can be extremely costly.

This includes damage to and theft and destruction of data, lost productivity, money being stolen, the cost of actually recovering from the attack, and the intangible cost of reputational damage that a breach causes.

There is no doubt that South African organisations are and will continue to be targets of cybercriminal activity, and it is past time to take the threat seriously.

It is essential to implement as many controls as possible to prevent an attack, rather than waiting for an attack to occur and then attempting to mitigate the damage.

It is important to focus on the boundaries of an organisation with effective perimeter security, which should include mobile devices, end points, networks and so on.

While the cloud increases complexity by blurring the physical boundaries of an organisation, it does not change the principles of security.

Basic controls that need to be in place include a perimeter firewall, endpoint protection and antivirus, among others.

Critically, these controls need to be patched and updated regularly to ensure they continue to provide adequate protection to the latest security threats.

Email security is also essential to minimise exposure to infected links and attachments, phishing scams and other malicious gambits perpetrated over this medium.

However, threats do not always come from outside of an organisation and breaches may occur through human error without the involvement of any malicious intent.

Users may accidentally compromise a network, for example by connecting a mobile device to an unsecured network at a coffee shop, where they pick up a virus, and then connecting to the corporate network where the virus can now gain access.

Education must always form a significant component of any threat prevention solution.

Above all, as people we need to start acknowledging that protection solutions are not just random hoops to jump through that make life difficult.

They are put into place for a specific reason and are critical to our security.

In the past, the approach has often been to reactively detect breaches and then try and clean up the mess.

The nature of the threat, however, and the increasing cost of such an endeavour, make this approach ill-advised in the current and future landscape.

It is far less costly to prevent an attack from getting through in the first place, and new technologies are now available to help us do just this.

South African organisations have a history of underestimating the potential risk, and this is an attitude that needs to change.

■ Tassev is a managing director and qualified security assessor at Galix