SA companies under cyberattack?

By Chad Fichardt

11 Jun 2015

The speed of technological change is leaving gaping holes in highly sensitive company IT infrastructure. These vulnerabilities are being targeted by cybercriminals at an increasing rate as South Africa is starting to feel the heat from attackers across the globe.

It was revealed at the recent 2015 Security Summit, in Johannesburg, that South Africa is the most attacked country on the African continent over the past six weeks.

Organised cybercrime

sheelamohan via freedigitalphotos.net

Vernon Fryer, chief technology security officer at Vodacom, presented alarming statistics from the Vodacom Cyber Intelligence Centre revealing a 150% increase in the number of DDOS attacks in the last 18 months in Africa. These attacks occur where multiple compromised systems, usually infected with a Trojan, are used to target a single system causing valuable downtime to assets like websites.

A typical attack on South African assets averages 9Gbps and lasts 17 minutes. A large attack may last a couple of hours, according to Fryer. These attacks are not specific to any sector or organisation. Cybercriminals are adaptable and tend to follow the money.

Jason Louw, forensic cybercrime-fighter, maintains that "99% of all global phishing attacks originate from organised crime. The problem is that we've seen very few prosecutions in SA cybercrime."

Spear phishing attacks

Symantec's Antonio Forzieri says that one in 214 emails sent in South Africa last year was a spear phishing attack. Don't let the exotic naming fool you. These attacks can cause serious personal distress, financial loss and are achieved by the simple click of a malicious link in an email.

Interestingly, the effectiveness of a spear phishing attack rises from three to 70% when private personal info is included. Most times this information is accessed easily online or hacked through open source websites," says Ignus Swart from the Council for Scientific and Industrial Research.

It is no wonder then, that cybercrime statistics recently posted by the South African Banking Risk Information Centre show that South Africans lose in excess of R2.2 billion to internet fraud and phishing attacks annually.

Are South Africans sufficiently protected by legislation?

It is a little-known fact that only 28 countries in the world currently have a cyber security policy in place. South Africa is one of them, but its policy is heavily criticised.

Professor Basie von Solms, director of the Centre for Cyber Security at the University of Johannesburg, says a single point of contact is needed for cyber security in the South African Government.

"The AU Convention shows SA is far behind as far as cyber security is concerned. Government and private sector must work together to cyber secure SA." he added.

Is it all doom and gloom?

There are those that believe that we can win. Hacktavist-turned-security-expert and Gigaom Research analyst, as well as recent TED Talk speaker, Keren Elazari, says the answer lies in decentralising the current systems.

"When it comes to the global financial ecosystem we are at a massive shift point, moving from traditional 20th century finance that is centralised to a new financial world with micro-payments, digital payments, digital wallets, crypto currencies and other forms of payments."

Elazari is convinced that as this change occurs it will empower small companies and individuals to have a bigger say in their own cyber security.

Vigilance is key

Mustapha Zaouini, CEO of payments company PayU, explains that as payment ecosystems develop, the threat of attack from unsuspecting sources such as third parties will increase.

"It is going to get very complicated for the ordinary business to keep track of all the innovation to thwart cybercrime. So it is vital that basic security measures are in place and that online companies keep things as simple as possible. We have seen this among our small to medium-sized merchants. The more aware you are of the risks, the more secure your online assets will be. Vigilance is key."

According to van Solms, small businesses are reported to be the largest growth area for cyber attacks, adding 31% of all attacks targeted small businesses, as they are less prepared to handle cyber risks. Another reason to use providers who are credible.

"Our payment systems are secure in South Africa, however, security is a culture that needs to be integrated into our daily lives. This applies to small and large companies as well as individuals and starts with password management," says Zaouini.

This year's Security Summit highlighted that while tenacious attackers and equally dedicated IT security companies compete for the latest technological dominance, all we can do is play our part with common sense when it comes to privacy and online security.

ABOUT THE AUTHOR

Chad Fichardt, senior PR account director at Media Web