BIZCOMMUNITY

What will the cyber threat space hold in 2017?

By Riaan Badenhorst

10 Jan 2017

"If only I knew then, what I know now!" seems to be the mantra of far too many organisations in the ever-evolving cyber security landscape. In fact, in our experience, we have noticed that today, many companies seem to be spending approximately 80% of their security budgets trying to prevent security breaches, while only 20% is being used to predict, detect and respond to attacks.

The reality, however, is that those organisations who have suffered a security breach, understand that this 'reactive' approach to cyber security is no longer effective, given pace at which the cyber threat landscape is evolving.

Looking back at the cyber threats predicted for 2016, which included seeing more players entering the world of cyber-crime, significant evolution in cyberespionage tradecraft and a dramatic change in how APTs are structured and operated, unfortunately most of these did surface, and further to this, 2016 has be declared 'the year of ransomware'. In fact, according to our research on ransomware, 20% of all businesses across the world have experienced a ransomware attack in the last 12 months.

In South Africa, this figure sits at 19%, which shows just how many companies are becoming victims and are paying to get their data back. Turning our attention to 2017, and the below predicted threats, it will likely be a difficult year, especially for organisations that only have security solution as protection. The main theme of 2017 is the growing ability of attackers to customise, hide, disguise or manipulate evidence and indicators – making it ever harder to spot and correctly identify them.

A rise in vigilante hackers: It has been predicted that cyber criminals will look to hack and dump data, which is allegedly done for the 'greater good'. This can mean businesses and reputations are compromise if targeted.

Espionage will go mobile: Espionage campaigns, which can also be a serious threat to businesses, will look to target primarily mobiles, benefiting from the fact that the security industry can struggle to gain full access to mobile operating systems for forensic analysis.

Device integrity in an over-crowded internet: As Internet of Things (IoT) device manufacturers continue to develop devices that are not necessarily protected, which can then cause wide-scale problems, there is a risk that vigilante hackers could take matters into their own hands and disable as many devices as possible.

Phases of IT security

Considering these predicted threats, cyber security should be everyone's priority, and local companies, no matter their size, need to change their 80/20 approach to IT security – and become more proactive. To best understand what this strategy needs to look like, a business should examine the security process itself, and gain an understanding of the four distinct, universal phases of IT security.

Threat prevention: Here a business needs to examine how it can block all the generic threats, which are emerging. It doesn't sound like much, but our research shows the generic threats emerge at a rate of 310,000 a day.

Detection: This phase requires advanced tools and expertise, as well as the time to identify the indicators of attack, spot an incident, investigate it and mitigate the threat.

Responding then becomes crucial – which businesses must not ignore. This phase requires the unique skills of forensic experts to ensure that the response is effective and that the threat is dealt with, entirely.

Prediction of future attacks means understanding the attack landscape of today, to assist a business in determining the long-term strategic defense required.

Of course, technology alone cannot protect a company. However, efforts from all departments must be unified and every department must know the company IT security policy to avoid falling victim to such predicted threats.

ABOUT RIAAN BADENHORST

Riaan Badenhorst joined Kaspersky Lab in January 2011. He headed up the corporate sales division, focused on growing Kaspersky Lab's market share in both the Enterprise and SMB sectors in sub-Saharan Africa. In October 2012 Badenhorst was appointed as managing director for the Africa region and has been heading Kaspersky Lab operations in the region ever since.

- How many abandoned online accounts do you have? - 14 Feb 2020
- #BizTrends2018: The developing cyberthreat landscape - 15 Jan 2018
- #BizTrends2017: What will the cyber threat space hold in 2017? - 10 Jan 2017

View my profile and articles...