BIZCOMMUNITY

Protecting the enterprise from evolving cybercrime attacks

By Saurabh Kumar

17 Apr 2015

High-profile cyber-attacks on blue-chip global companies have sent shockwaves around the technology industry. It's clear that threats in the digital era are morphing - becoming ever more sophisticated and destructive...

In the past couple of years we have seen devastating attacks on the likes of JP Morgan Chase, Target, and MasterCard. These incidents compromised personal and financial data relating to tens of millions of customers. The most recent attack in the spotlight was that of Sony, involving the theft of critical data, and the leaking of confidential information.

In the US, President Obama recently highlighted the threat of cyber-security in destabilising corporations, and even entire nations, while shifting the issue of cybercrime to the top of his agenda for 2015.

Internal threat

These events have left local chief information officers (CIOs) wondering how they can protect their organisations from modern cybercrime tactics. However, while creating strong defenses against external threats is important, our recent In2IT survey revealed that 60% of security threats actually come from those inside the organisation.

This is a startling figure that many companies are loath to accept. However, the reality is that employees are the biggest source of malicious activity and confidential data leaks today. Vulnerability assessments, penetration testing, and security policies must all respond to the internal, as well as the external, threats.

South African companies also tend to suffer from a false perception that the threats and risks are minimal. While that may have been the case a few years ago, today the reality is that cybercrime is 100% global.

However, what can local firms do to shore up their defenses against the latest cyber criminal activity?

- Firstly, security policies need to be defined that respond to the current threats - too many organisations have policies that are no longer relevant. Then, it is crucial to ensure that the policies are enforced across the organisation.

- The issue of enterprise mobility needs to be comprehensively addressed. Approaches to mobility can range from the most limiting (employees cannot use their own devices for any work activities) to the most *laissez faire* (saying 'there's no use in stopping it' and implementing no restrictions on employees' own devices). Either of these approaches leave the organisation vulnerable. Implementing proper security policies on mobile devices helps to minimise the security risks

inherent in increased mobility.

- The use of two-factor authentication mechanisms - such as a passwords combined with a physical token-generator - should be the only way to access critical data, sensitive data, and financial data.

- Demilitarised zones ensure that as devices re-enter the network they do not carry any malicious software with them. Mandatory scanning and quarantining helps to ensure the organisation from these forms of threats.

- Using a series of virtual local area networks (LANs) throughout the organisation can help to segment the data into discreet areas (for example, having a V-LAN for different business units, or different regions). This approach helps to minimise the damage caused if there is a security breach, as it restricts the damage to just one V-LAN, and not the entire enterprise.

Security breaches cause the erosion of trust and customer confidence; they have a massive impact on the health of the brand and may well present direct financial consequences to organisations and their customers.

South Africa will certainly not be immune to the next wave of cyber-attacks. If some of the world's most prestigious financial organisations can fall victim to this form of crime, then the defenses used by many local companies will not withstand even the most casual attempt.

ABOUT SAURABH KUMAR

Managing Director at In2IT Technologies South Africa

- Digitisation and tech are key for businesses to thrive in 2021 - 8 Jan 2021
- The value blockchain can bring to business - 26 Jan 2017
- Digital change begins with business leadership - 14 Nov 2016
- ICT investment can help fuel SA's GDP growth - 3 May 2016
- Outsourcing vs insourcing: trust innovation to the experts - 25 Feb 2016

View my profile and articles...