Kaspersky Lab releases Global IT Security Risks Survey results

MOSCOW, RUSSIA / JOHANNESBURG, SA: 91% of companies globally have experienced an IT threat over the last 12 months according to Kaspersky Lab's Global IT Security Risks Survey. In fact, over the period, 61% of the attacks were due to malware infection, 48% of companies have noticed an increase in the number of cyber attacks and 30% of companies have lost critical business data.

These statistics aren't surprising if one considers that globally, 2 billion network attacks are blocked monthly, 2000 application vulnerabilities were detected in 2010 alone, 70 000 malicious programs appear daily and 1 new malicious program appears every second.

New threats emerge

Says Alexander Erofeev, head of Market Intelligence and Insight at Kaspersky Lab; "Each year, the industry of cybercrime evolves with new threats emerging at a pace that is almost impossible to follow. And from a business point of view, it is fast becoming, not just a must have, but a crucial element for future business viability."

From a South African perspective, the statistics mirror global trends:

- 79% of organisations surveyed have been attacked by viruses, worms, spyware and other malicious programs
- 39% have experienced data loss from malware attacks
- 43% of respondents currently see cyber threats as one of their top 3 critical business risks, while 53% see it as a developing business risk in the next 2 years
- What's more, 54% believe their organisation is under resourced in term of staff, knowledge and funding in coping with IT threats. Of this percentage, 91% say that 25% or more investment is required for security.

"In line with such statistics, it's interesting to note that many organisations are restricting social networking applications to reduce potential risks. What's more they are often reluctant to adopt new technologies because of the security risks," adds Erofeev. "In fact, South African statistics indicate that 67% of respondents are worried about the involvement of organised criminal gangs in cyber attacks and global incidents are prime examples of such threats - with the likes of the DigiNotar and Comodo hacks to name but a few."

The basis for solid security

A solid security solution is the basis of any success security strategy, but companies should not forget that an anti-virus protection must be complemented by a firewall, an intrusion detection system and a security scanner that can be used to find vulnerabilities in the system and can suggest ways to fix them. It is also important to have backups, which can be used to restore data in the case of a disaster. Additionally, tools allowing controlling applications, web content and removable devices raise the overall security level. Having a centralised management approach to security within an enterprise can assist in this being achieved. And of course - remember the human element. It is important to educate the users continuously about the dangers of cybercrime and how it can be avoided.

"Unfortunately, there is no foreseeable end to the growing cybercrime problem; on the contrary, numbers seem to indicate it is becoming larger from both a local and global perspective, which means that businesses need to exercise heightened online vigilance - ensuring security becomes and remains a key priority and concern. Remember, a healthy dose of scepticism will go a long way in helping to protect your business against fraud and scams: a reputable security solution and up-to-date software should take care of everything else," concludes Erofeev.