Think layers of security – and start with the physical

It takes more than security software to protect your corporate network, says Netshield.
Johannesburg, 16 February 2017 - As security vendors predict more focused and personalised cyberattacks in 2017, companies should consider multiple layers of security to protect their companies.

This is the word from Inus Dreckmeyr, CEO of Netshield South Africa, a Westcon-Comstor Southern Africa company.

“Even the best possible security software will not offer your business 100% protection against external threats, all of the time. Furthermore, security software also cannot protect you against all internal threats – nothing can. But a comprehensive implementation of several layers of security, starting at a physical level in your organisation, will at least alert you to an attack early enough to do something about it,” Dreckmeyr says.

He believes that many companies become complacent once they have installed security software. They then tend to forget, he says, that the phenomena of bring your own device (BYOD) - including something as innocuous as a promotional memory stick - combined with more broadly available connectivity, makes corporate systems more vulnerable than they have ever been to insider attacks.

“An insider attack needn’t be a malicious employee - it could simply be an employee who has downloaded the latest game on their smartphone. If that software has a piece of malware included, and the employee has access to your corporate network via their cellphone, the malware could populate your network in seconds,” he warns.

“You have to protect the base and foundation of your network at all times. One way to do it is to protect each layer separately. View the physical components, as well as the software and endpoints within your network as individual "things", and then layer your security approach to each. You will not only have better management and control of each layer, but better security as well. If you follow this more layered approach you can then start applying solutions such as a proper access system at a granular level. This then allows you to monitor exactly who is working on any aspect of the network at all times.”

Dreckmeyr says that while passwords are still a good deterrent, they offer little protection. “If John, your marketing director, leaves the office for a meeting without logging off, his machine and the network are both vulnerable. If, however, John’s network access is automatically logged out the minute he swipes his physical access card to leave the building, there is an added layer of protection.”

If we assume that there is very little that will actually protect your company from cyberattacks happening, Dreckmeyr believes that monitoring and linking physical access can make a huge difference to a company’s response to one of these attacks. In the above example, the network administrators would be alerted that John’s machine is accessing the network, even though John is out of the office. This allows the IT team to investigate the threat, shut down John’s machine remotely and stop a potential breach in its tracks.

In his experience with the companies he has assisted, employees understand that this is a global trend and they generally do not take offence at being monitored and tracked in this way. “People know that everything they do on their smartphones is being tracked by someone – even if it is just using Google. Extending this tracking to a scenario that ultimately makes their jobs safer, by safeguarding the company’s core business, is unlikely to upset a rational worker.”

Dreckmeyr suggests that companies do “black box thinking”, and look at every possible layer of security on their network, not only the software layer. “Keep asking yourself ‘how secure is this really?’, and build layers of security around each process,” he adds. “When it comes to networks, the first layer should always be physical, bearing in mind that it is not good enough to control only who logs in or who accesses the building. Companies should also control who has access to their network, server room and who has access to the server cabinet that houses their core network infrastructure, and which logins assigned to users in the business can make critical changes on the core network.”

This is where products like Netshield’s NVIROMON-1S come into their own, Dreckmeyr says. The NVIROMON-1S is not just used to monitor and control the conditions inside a room, detecting heat, humidity, gases and fires, as well as power outages. You can very easily and effectively ensure that your NVIROMON-1S provides you with additional security layers that ensures complete control of who has entered and who has logged into the network with physical security to server rooms and network devices, thus providing an additional simple but effective layer of security for businesses.

“With the NVIROMON-1S you can detect and proactively react via an easy-to-use dashboard. What’s more is that the NVIROMON-1S will proactively alert you via SMS or email if you aren’t within the direct vicinity of your management console,” he says.

In the process, it delivers an additional simple - but very effective - security layer for businesses.