

Network Box advisory: 'Forgotten Security'

Part 1: Monitoring

In the first of our advisory notices on 'forgotten security', we advise companies to monitor their applications, hardware and security systems to protect against vulnerabilities resulting from insufficient monitoring.

Companies are protecting themselves from high-profile threats such as malware attacks, but are often leaving themselves vulnerable from the 'forgotten security defences'. The first of these results from simply not monitoring the applications, hardware and security systems across the business, which can lead to network failure.

Most businesses are using an increasing numbers of applications, including web-based applications. This has led to a greater number of SQL Injection attacks (injecting code into a trusted application to make it do something it shouldn't), which we wrote a separate advisory on recently, and which you can find here: <http://www.network-box.co.uk/aboutus/news/network-box-warns-companies-take-action-against-increase-sql-injection-attacks>. We are also seeing serious vulnerabilities in 'social' or rogue applications that are creeping into businesses, (such as P2P software – see our guidelines on this here: <http://www.network-box.co.uk/sites/default/files/nb-guide-to-p2p-security.pdf>) that are often inherently insecure, as they are not built with business purposes in mind.

Our advice to IT managers is to review the number of applications used across the business regularly, and test them for vulnerabilities, failures and correct use by employees.

The following actions should be undertaken regularly:

- Review all applications regularly and test them for vulnerabilities and correct operation
- Check that all security processes are actually running. Ensure they are updating effectively, and scanning properly. Check what is being scanned, and whether any changes have occurred as a result of system or user errors
- Check continuously that you are not sending out viruses or spam from within the organisation
- Monitor VPNs to see that they are up and providing connectivity between offices
- Check the firewall configuration is correct and is patched with the latest version
- Check for intrusions like username and password retries
- If a server has hard disks, ensure there is an effective, working system in place to see if it is generating hard disk errors indicating that it might fail
- Monitor CPU temperatures: a system running hot will reduce its life span, reducing ROI
- For the same reason, check fans. If they stop, then areas of the motherboard may not be cooled efficiently, causing the system to fail or to work in a stressed fashion reducing lifetime of the system. The same applies with power rails
- Check for network errors where routers and network cards are not using the optimal settings or failing to negotiate with each other and hence network speeds are poor reducing productivity
- Check how busy your system is. Is it reaching its maximum throughput, and is a bottleneck reducing productivity?

In addition, we suggest taking the following steps to ensure optimal working of applications, hardware and security:

Monitoring applications:

- Monitor your users and review the applications they use as part of the ISO9001 process or about once a quarter. Set clear user guidelines and policies covering which applications can and which can't be used within the business, and how, and enforce that policy

- Test for vulnerabilities in applications. You can use automated systems, such as securityspace.com that do perimeter tests for you
- Ensure that you have a way of checking if operating systems and applications have been patched. Secunia.com provides a free service that allows you to run a test and find out what is not up to date

Monitoring security systems:

- Always consider what security systems you need, how you are going to monitor security, and what needs to be monitored, when you put it in place

Monitoring hardware – warning systems

- Agree at what point a warning becomes critical and implement a warning system that you can monitor effectively. For example, you might chose to receive a warning if the CPU temperature on a piece of hardware reaches 40, but a 'critical' alert when it reaches 60, depending on the hardware in question
- Ensure there is a system in place to alert you to warnings: by email, screen or sound, or all three
- If you are monitoring a large number of devices consider the server load. Monitoring can become quite processor intensive if mishandled or misconfigured

For more information on the latest security issues, see <http://www.network-box.co.uk>, or visit Simon Heron's blog at: <http://blog.network-box.co.uk>, or follow Simon on Twitter: <http://www.twitter.com/networkbox>.

About Network Box:

Network Box Limited (NBL) is an international managed security services company, specialising in unified threat management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread around the globe. NBL's customers in Asia, Australia, North America and Europe include companies such as BMW, Nintendo and Toyota, as well as banks, utilities companies and government organisations.