BIZCOMMUNITY

Don't trust employees with securing data on the prowl

Companies cannot trust security of data on the prowl to employees. Data security remains the responsibility of the IT department - and this requires extending data visibility and control beyond traditional perimeters.

Image: www.freedigitalphotos.net

"Today, almost every employee in the average corporate has the ability to work on the move, using his devices of choice and generating and processing company data from wherever he is. The trouble is that in many companies, users are literally left to their own devices when it comes to security.

"It is not safe to assume that the security software on laptops is configured correctly, that it is updated, or that no changes have been made to make the system vulnerable. Not everyone is aware or as diligent about IT security as we would hope. Even the basics like firewalls, anti-virus and anti-spam are being neglected, and users are plugging in peripherals into assets that store critical business information without restriction. This exposes company information to risk.

"Smartphones and tablets in particular are not governed nor monitored, which means that they can introduce network threats and negatively impact on an organisation's compliance status," said Richard Broeke, from IT security vendor Securicom.

A tricky line

He said that IT departments now have to walk a tricky line to meet users' expectations for immediate data access on a choice of devices, while protecting the organisation's information assets. But, whether it's about managing devices like tablets and smartphones or managing an ecosystem of desktops and laptops, the key is to have a central point of control.

"With a myriad end points and devices at play, the conventional approach of installing and managing different point security solutions on each end point just doesn't work. What companies should be able to do is manage the entire lifecycle of all the end points and devices in the enterprise from a single point. This includes commissioning new end points and installing, monitoring and updating the necessary security technologies, right through to decommissioning," commented Broeke.

An effective, centrally managed end point security solution will help to ensure that security updates are routinely applied and that authentication and access rules are enforced. It also offers the ability to limit or prevent the use of peripheral devices on company computers, as well as implement mechanisms to control which applications and business information certain levels of employees are permitted to access.

When rules are broken, company resources are abused, or security on a device is outdated, the administrator can be alerted and can take action to remedy to problem.

A centrally managed end point security system also assists with the effective, efficient and safe on-boarding and decommissioning of company assets. It's not difficult to replace a laptop, but recovering the exposed information is.

Likewise, an effective, enterprise mobile device management solution will allow companies to secure and manage a diversity of smartphones and devices from a single point - even in a Bring Your Own Device scenario.

You can't leave it to users

"To protect against mobile threats effectively, companies need to have the ability to configure and provision devices, enforce security software updates, manage access to company resources from mobile devices, monitor device compliance and decommission devices. This should include the ability to wipe clean mobile devices that have been lost or stolen. None of this can be left up to users," he said.

But this doesn't mean employees can abdicate all responsibility for data security on the devices they use to work.

"With most privileges comes an obligation. To enjoy the privilege of accessing and working with company data outside the office, employees must understand that they have an obligation to follow the organisation's required security policy guidelines. Employees should be aware of security processes and procedures and the consequences of disregarding them," concluded Broeke.