BIZCOMMUNITY

BYOD security still lacking

Most companies today have implemented bring your own device (BYOD) strategies, that allow their staff to use their personal devices, whether tablets or smartphones, at work. However, a recent BitDefender survey has revealed that BYOD policies, aimed at securing personal devices, and the business data stored on them, are not nearly as comprehensive as they should be, and have a way to go if they hope to protect the business effectively.

Lutz Blaeser

BYOD is no longer a trend

The study was carried out by Millward Brown, and spoke to 1,045 US-based internet users aged 18 and up, carried out in August last year. Lutz Blaeser, MD of Intact Security, says the results should shock organisations into reevaluating their BYOD policies, and ensure they are both up-to-date, and thorough enough to safeguard a company's most valuable asset - its information.

"BYOD is no longer a trend, it has become the de facto way many employees do their jobs. The idea of connecting personal devices to the corporate network is now widely accepted, and the majority of staff are taking full advantage and using their own smartphones, phablets and tablets to conduct business."

The greatest offenders

He says the concern is that these employees are storing business-related information on these personal devices, even when the business has no BYOD policy in place.

"This isn't even the most dire revelation. When those surveyed were asked how these personal devices are secured, just under a third claimed to make use of a personal identification number (PIN), while not even half employed a complex password. Around 40% claimed to have absolutely no security measures in place to prevent unauthorised access to their phones and tablets."

The survey also revealed that staff aged 30 to 44 were the greatest offenders when it came to the lack of passwords, choosing to rather use biometrics or swipe patterns to lock their phones.

Wipe the device

He says given the lackadaisical attitude that most employees seem to have towards BYOD, having a good policy in place, combined with a robust mobile security suite, is key. "When dealing with any device that stores business information, having the ability to remotely wipe any sensitive data should the device be stolen or lost is vital. This is even more important given that the survey shows that the majority of people are either unaware that there is the ability to remotely wipe a device or they haven't switched the feature on."

For businesses, both large and small, the implementation and management of mobile security software is often expensive and uses too many resources, Blaeser adds. "As threats grow in intensity and sophistication, businesses all over are finding it harder to protect themselves and their business assets and stay ahead of the latest threats. However, this needn't be the case."

He says Bitdefender Security for Mobile Devices has adopted a holistic mobile security approach that helps businesses maintain compliance while keeping IT intervention to a minimum. It is not just another solution that adds to the workload of administrators, as it utilises a management platform that is also used for controlling security across virtualised and physical endpoints. Companies can start enforcing security policies to mobile devices in no time, without any additional infrastructure required."