BIZCOMMUNITY

BYOD: risks, policy and management

Bring Your Own Device (BYOD) has been a hot trend for some time now. More and more workers are using their personal cellphones and tablets to access company data. In fact, Gartner predicts that by 2017, 50% of businesses will require their staff to supply their own devices for business purposes.

©kantver via 123RF

While this may seem to benefit both employers and employees, this is not necessarily the case, says Lutz Blaeser, MD of Intact Software Distribution.

“Mobile malware is growing exponentially, and it is mostly going after Android users. Moreover, most mobile applications do not have even basic business-class security measures in place. The fact that wearables are becoming an integral part of enterprise mobility strategies is only going to compound the issue.”

Mobility risk

He says a growth in mobility means a growth in risk. “Over and above malware, increased mobility means there is a better chance of having a mobile device lost or stolen. This is a major concern for businesses with regards to mobility. The more devices of all makes and models that are used to store and access business data, the more vulnerable they are to mobile security threats.”

There is no doubt that although BYOD has numerous benefits in terms of productivity, time saving and similar, it is also putting a great strain on the organisation's data security, he adds. "The true costs of a data breach goes way beyond the costs involved with replacing a device, or even the costs to implement BYOD. This is why organisations must widen the scope of their BYOD policies to cover all types of devices and applications used by staff, and more importantly, put data security at the core of these policies."

He says there are several key features to any mobile security solution. "There are the obvious mobile device management functions such as wipe, lock and track a device remotely, but these are no longer enough to protect data travelling through different channels – off a device, through USB ports, email and all kinds of applications, into the cloud."

BYOD policy

Over and above these basics, a strong BYOD policy must cover core security functionalities to allow a company to build on them, should such measures be needed in the future.

Blaeser says there are five core security functionalities a strong BYOD policy needs to check. "Firstly, data encryption, for data residing on the employee's device and for data transiting different channels. Next, application access control, which employs policy-based firewall as well as intrusion prevention and detection. Mobile malware detection and removal, is also an essential element, as this will make sure clean devices enter the organisation, and remain free of any malicious software while they are in use."

He adds that real-time application and website scanning, to guarantee the device doesn't pick up any infections through malicious applications or websites when the staff member wants to download or access them, is also a necessary component.

"Finally, application permission management, to enable employees to see the types of information an application asks permission to access and share with the application vendor. Too often applications ask for access to information they really shouldn't need at all. Employees need to understand the dangers."

A good mobile device management (MDM) solution plays a crucial part in any BYOD policy. If core security functionalities are not integrated into your MDM solution, you really should consider getting them, Blaeser says. "Don't merely manage the device or the applications, when the application permissions can be managed too. Also, go beyond management functionalities, and add a mobile anti-malware engine to ensure solid mobile protection. Look for a solution that offers all of these elements."