Securing mobile access to your organisation

When designing their mobile security policies, there are several issues security professionals need to bear in mind. Businesses are using smartphones and tablets to access sensitive company data, and as such, need to be protected.

Lutz Blaeser

Probably the most common application accessed by mobile devices in the workplace is company emails, says Lutz Blaeser, MD of Intact Software Distribution. "Corporate emails often contain highly confidential data, which can also be subject to compliance and privacy regulations."

Myths surrounding mobile security

He says despite the fact that businesses are aware that securing the mobile platform is vital, many businesses battle when it comes to planning, designing and implementing BYOD policies. "This is often due to several myths that surround mobile security."

"Probably the most dangerous of these is that mobile device users don't really believe that critical information is accessed via their devices. Either that, or they believe that since their access to company data through their smartphones is so infrequent, it minimises the threat surface to a point where it can be considered negligible," says Blaeser.

"However, mobile access and use is ubiquitous, and there is a lot of data cached in today's devices, either in emails or in files. If these files and mails are not secured via either encryption or access control, they can easily fall into the wrong hands."

A fatal flaw

One fatal flaw, he says, is the belief that password management, biometrics or PINs are enough to prevent sensitive data from being stolen. "We all know how hard it is to remember passwords, particularly given that we are required to remember numerous ones for every card, website, online store and suchlike. Unfortunately, because of this, too many people write them down, which kind of defeats the purpose."

watcharakun via freedigitalphotos.net

Another significant danger, says Blaeser, is the notion that app stores, such as Google Play or the Apple App Store are safe, and do not allow any dodgy apps to make it on to the sites. "Unfortunately, all apps are not vetted, checked for malware or verified. A good rule of thumb is to check app reviews from other users to get a real idea of what they are like, and always check with permissions the app requests. Don't download apps that ask for permissions that they would have no legitimate use for."

Blaeser adds that there is an alarming trend of people believing that an anti-virus for their mobile phones is unnecessary. "Nothing could be further from the truth. Bitdefender's mobile security product addresses all these issues and many more. Its Privacy Advisor tool gives you detailed information as to what your installed apps are doing in the background without your knowledge, preventing your personal information from being abused. Its anti-theft feature provides options to remotely locate, lock, wipe or send a message to the device, and its App Lock allows users to surf the internet and socialise without worries, as personal information cannot be seen or stolen by hackers."