Balancing mobility risk with data availability requirements

Mobile devices have become an integral component of the Always-On enterprise. But what impact do they have on the modern data centre, especially when employees expect to have access to mission-critical data from wherever they are? Rick Vanover, senior product strategy manager at Veeam, takes a closer look.

Rick Vanover

“We are living in a connected world. People are using a number of smart devices to remain in touch with not only family and friends but also with their employers. This flexibility gives them the ability to access vital data whether they are in the office or watching their children compete at school sports,” Vanover says.

The move to mobile

According to recent figures, even the South African market is embracing the shift towards smartphones. With 37% of people indicating they are using the devices, the opportunities for the Always-On enterprise are significant. Improvements in productivity aside, the ability to leverage data as close to real-time as possible means decision-makers can gain vital insight while ‘in the field’, giving them a crucial competitive advantage.

Furthermore, the 2016 Veeam Availability Report has found that 73%of South African respondents indicated that the increasing adoption of mobile devices is a key driver for minimising application downtime and guaranteeing access to data. But with this embracing of a more mobile way of doing business comes concerns around the security implications.

“From a mobile security perspective, there needs to be automated processes implemented similar to what happens inside the physical boundaries of the office. Take for example when a person leaves the enterprise; their access to the network is automatically revoked. But what happens to their mobile access? Often, this is a critical step that gets neglected,” says Vanover.

Ensuring such an authorisation framework is active usually falls within the responsibility of a solution like Microsoft Active Directory which has a consistent authentication mechanism in place. But for this solution (and others) to work, the enterprise needs to make certain that the link to it is available. In keeping with the premise of Always-On, if this is not the case, then the company is open to serious security risks.

Kaboompics via Pixabay

Device management

“The moment authentication is unavailable, an enterprise seriously impacts the security of its data. Despite this, mobile apps are not going away. Enterprises need to implement a rule-set in their modern data centres that reflect the changing requirements. Such a rule set could also counteract the risks of using consumer software in the business environment,” Vanover adds.

The file-sharing phenomenon is a prime example of what happens when employees get comfortable in using consumer solutions in the business. While the enterprise might have the best systems in place to protect their data, not much can be done once an employee shares that over a service like OneDrive or DropBox.

“The moment people have access to back-end systems on their phones they could compromise its security by using these and other third-party apps. In this instance, the best strategy then would be to utilise mobile device management as a way to secure the link between mobile devices and the data centre.”

Features of such an approach include the ability to remotely wipe the data off a smart device if it gets lost or stolen. But this on its own is not enough. Policies and processes need to be updated to reflect the growing role the mobile device is playing inside the enterprise.

“All of this points to the need for the Always-On enterprise to link data between mobile devices and the data centre. Decision-makers need to re-examine data hierarchy and its importance in the context of security and trust zones,” concludes Vanover.