New ways to combat BYOD

By Ernst Wittmann

10 Nov 2015

Many employees are doing their work from home and executing an increasing number of transactions on mobile devices. They make less use of their desktops and notebooks. This means that hackers and malware authors are increasingly focusing their efforts on mobile operating systems and ecosystems, in addition to attacks on traditional PCs.

Ernst Wittmann

This according to Ernst Wittmann, Country Manager Southern Africa for Alcatel OneTouch, who adds that companies need to put in place a coherent mobile information security policy as well as a robust mobile device management environment to keep their information and applications safe. "We're seeing a shift in the working world as people start to use their smartphones and tablet computers for mission-critical tasks, ranging from on-site customer service to online banking," says Wittmann. "Now that our mobile devices have access to banking logins, enterprise resource planning systems, sensitive financial data, and customer database, they are attractive targets for cyber criminals and thieves."

Against this backdrop, responsible companies need to have a coherent plan to respond to threats such as the theft or loss of a physical device, hacking attempts, and mobile malware, he adds. This is especially important with the Protection of Personal Information Act and other laws and regulations prescribing tough penalties for companies who don't take reasonable steps to safeguard customers' personal information.

BYOD trend is hard to reverse

kaboompics via pixabay

Wittmann notes that the shift towards mobile work has introduced a range of complexities to corporate information security, starting with the fact that many of the devices used to access company applications and data are user-owned. CIOs need ways to ensure that such devices have appropriate security, he adds. Though some companies are pushing back against the Bring Your Own Device (BYOD) trend, implementing Company Owned Personal Enabled (COPE) and Company Owned Business Only (COBO) models is difficult in practice, says Wittmann.

Users are reluctant to give up their own SIM with their phone number, the apps they love to use, and their platform of choice in favour of a company standard. Trying to crack down may lead to rebellion and shadow IT. What's more, IT

doesn't have the power to dictate what smartphone the CEO or sales director should use. In addition, trends such as the rising use of outsourcing partners and contractors, and growing reliance on cloud apps makes it difficult for CIOs to take complete control of devices and apps in their end-user populations, Wittmann adds.

"Consumer devices and apps are vulnerable points in the corporate IT environment since they're easily lost or stolen. A physical device ending up in the wrong hands is still the most significant mobile security risk, despite growing volumes of mobile malware," he says "Whether they put in place a BYOD, COPE, or COBO strategy, companies need necessary policies and controls to mitigate these risks. Luckily, the tools to manage BYOD have evolved over the past few years, enabling companies to lock down security while allowing users to be productive on their own devices."

Keeping it contained

Wittman says that mobile device management tools enable companies to protect enterprise data and applications, even when they're accessed using an individual's own handset. These tools simplify management of devices across platforms - including iOS, Windows, Android, and BlackBerry - and ownership models. The solutions enable IT administrators to manage, provision, and activate devices, administer controls, push mandatory applications, and more.

Containerisation, meanwhile, creates a dedicated work profile on smartphones that isolates and protects work data and apps. End-users can use their personal apps knowing their employer only manages work data and can't erase or view their personal content. Google's Android for Work containerisation technology, for example, delivers secure mail, calendar, contacts, documents, browsing and access to approved work apps as an integrated part of Android 5.0, Lollipop devices.

mGoogle Play for Work, meanwhile, allows businesses to securely deploy and manage apps across all users running Android for Work. Google has extended access to Android for Work to older versions of the mobile operating system with an app. It has also partnered with mobile device management partners to give organisations a simple way to manage devices on a single console.

"With 10,000 companies in the US - including institutions such as the US Army and World Bank - using Android for Work, it's safe to say that Android is now an enterprise-class platform in terms of security," says Wittmann. "Companies now have practical ways to address their security concerns and manage devices across the whole mobile ecosystem."

ABOUT THE AUTHOR

Ernst Wittmann, Country Manager Southern Africa for Alcatel OneTouch