Feature

Let's Get This BYOD Office Party Started

01 May 2012
Fred Donovan

The most dangerous security aspect of BYOD, according to many experts, is the apps that personal devices run, not the operating system or hardware. Fred Donovan examines how organizations can say 'yes' to employee-owned devices while still maintaining control of their data

The firm's chief executive just got a new iPad as a Christmas present, and he wants to bring it into work. He is impressed by the features and the flexibility it gives him to perform his duties.

So he calls up IT and tells them he wants to use his new iPad to access the corporate network to send email, enter calendar items and contacts, download web applications, and a bunch of other things. And, of course, he wants to do all these things securely.

"But sir, our policy is not to allow personally owned mobile devices on the corporate network because of security", replies the chief information security officer (CISO). Or should we say the former CISO, because CISOs who want to keep their job are not going to give that response.

So what is a CISO to do? Bite the bullet and figure out how the CEO can download web applications without endangering the entire corporate network? If the company does allow employees to bring personal mobile devices to work, the security problems multiply exponentially.

"According to a survey by Proofpoint, 84% of organizations are allowing employees to use consumerized IT, but only 51% have implemented a security strategy to cover its use."

Failing to Plan

A security strategy or plan is essential to prevent the bring-your-own-device (BYOD) trend from becoming bring-your-mobile-malware to work, according to security experts consulted by *Infosecurity*.

Chenxi Wang, vice president and principal analyst for security and risk at Forrester Research, stressed that companies need to have a plan in place to manage the risks posed by personal mobile devices in the workplace.

Smartphone buzz kill: The most dangerous security aspect of BYOD, according to many experts, is the apps that personal devices run

Share

More services

Related Links

Infosecurity Magazine Interviews Good Technology

Elsevier Ltd is not responsible for the content of external websites.

Top 5 Stories

"With bring-your-own-device there is very little control over where corporate data can go", Wang notes. "That represents a big risk for organizations that are concerned about confidential data, and they often don't have a good policy saying this is where the data can go and this is where it cannot go."

"In order to exert controls, you have to give up some of the user experience", Wang continues. "For example, you could use an enterprise-wide solution to control whether employees can save email attachments on their device. In order to do that, you have to use a separate email client, so the users are not using their native email client.

"Some organizations elect to use only policies. They write a policy, 'Thou shall not do this', and communicate it to employees without using a technical solution to enforce the policy", Wang adds.

A lot of organizations are embracing BYOD because it can save them money by not having to buy their own hardware, observes Kevin Johnson, mobile security consultant with Secure Ideas and co-chair of the SANS' Inaugural Mobile Device Security Summit being held March 12–15 in Nashville, Tennessee. "But they are ignoring the security issues, such as how do you control these devices", he adds.

"If I bring my iPhone into work and you tell me, 'For the security of the organization, we are not going to allow you to install apps', my response is likely to be, 'This is my phone, and you can't tell me what I am allowed to do with it'", Johnson asserts.

When employees mix corporate and personal email on their personal mobile devices, there is a risk of confidential data leakage. Johnson related an incident in which he received confidential data from a friend who worked for a competitor. The friend had accidentally sent the confidential information to her personal contact list and because it was sent from a commercial email service, the corporate server protections that would have caught the confidential data were bypassed. He deleted it without looking at it and notified his friend of the error. "This kind of stuff happens with organizations very often...There are data loss risks, malware threats, and all of these other things that are happening with BYOD, and the organization has much less control".

Marketplace Security

The threat to organizations from personal mobile devices is exacerbated by insecure application marketplaces run by the mobile device providers. The two largest mobile app stores are Apple's App Store and the Android Market.

The consensus among the security analysts is that Apple does a better job at weeding out apps with malware before they get to the App Store, while Google is seen as reacting only after the malware has been discovered in the wild.

"Apple has fairly tight control of the applications that appear in their App Store, meaning that app developers have to be authenticated and purchase a license from Apple, and everything they write has to be signed by Apple", Wang relays. "Apple reviews the application to ensure that there isn't any malware. So far, they have done a pretty good job."

Android, on the other hand, takes a very liberal approach to applications that appear in their marketplace. They do not have an extensive review process", Wang concludes.

McAfee Labs researcher Igor Muttik shares Wang's skepticism of Google's app review process. "On the Android Market there is a constant trickle of unwanted applications".

In a recent white paper, Muttik attributed the poor security performance of the Android Market to a reactive approach to malware on the part of Google, as opposed to the proactive approach taken by Apple.

"Apple's approach is proactive and focused on prevention. Google's plan is apparently to encourage the creation of apps and deal with the problems as they occur, in a reactive fashion. Google's may be a sensible move to generate a large volume and wide variety of apps, but from the security perspective, it creates exactly the kind of environment in which malware gangs feel comfortable", he wrote.

> **"In order to exert controls, you have to give up some of the user experience"**
>
> Chenxi Wang, Forrester Research

Perhaps in response to Android's growing reputation of being a malware cesspool, Google unveiled in February the Bouncer automated application scanning service to root out malware on the Android Market. Bouncer performs a set of analyses of Android applications, whether new or already on the Market, as well as developer accounts.

What's an Organization to Do?

All this malware hiding in mobile phone apps creates particular worries for IT administrators when the mobile devices are used to access the corporate network. Malware on personal devices can result in the theft of confidential data or disruption and damage to the corporate network.

"When employees buy the devices themselves and bring them into work, they are bringing a big wad of malware in the front door", cautions Idan Shoham, chief technology officer with Hitachi-ID.

One solution is for the organizations to buy the mobile devices for the employees so that they can control the devices and load whatever security software they think is appropriate. "That's an expensive strategy", Shoham observes.

Organizations could ban personal mobile devices altogether. "For most organizations, that argument is not going to win", SANS' Johnson asserts. "The business is going to look at the cost savings from not buying phones. The executives are going to like the idea that they can bring their brand new mobile device to work."

Organizations can use a containerized approach to secure corporate data. This is a solution offered by Actividentity and Good Technology, notes Philip Hoyer, director of strategic solutions at identity management vendor Actividentity. He explains that his company has worked with Good to create an "enterprise container" on the mobile device. The corporate apps and information sit in a sandbox separate from the personal apps and information on the device.

Another solution is to use mobile device management to enforce security policies on personal phones. Companies need to be able to manage personal mobile devices, particularly if employees have corporate information on them, says Kevin Haley, director of Symantec Security Response.

> **"From the security perspective [the Android Market] creates exactly the kind of environment in which malware gangs feel comfortable"**
>
> Igor Muttik, McAfee Labs

The concern is that an "organization's information is going to go from inside the organization to the phone", Haley warns. "We have erected firewalls and physical security to keep our information in, but now it is going out on the cell phone...You have to assume it is in the hands of somebody it shouldn't be in if it is lost or stolen."

Haley recommends that organizations implement policies and procedures to track what devices are on the corporate network and to manage those devices.

At the same time, firms need to educate employees about the mobile device security policies and the risks associated with BYOD. "It doesn't do any good to write a policy. The end users have to understand it, and it has to work for them", Haley adds.

Muttik says that in the future, mobile devices might have the ability to separate access to corporate and commercial networks into two virtual systems. "We are not quite there yet on the technology front...Computing capabilities are growing all the time so it is bound to happen."

Shohan relates that IT shops are working with virtual desktop infrastructure for mobile devices. "What they are saying is, let me stand up a Citrix server or a terminal server type of environment. Sure you can use your device, but really it is just a thin client that connects to the device we own."

The bottom line is that personal mobile devices in the enterprise are here to stay. Technology might provide part of the solution to improve security, but the best strategy for enterprises is to make mobile devices as secure as possible through strong security policies and education.

This article is featured in:
Application Security • Compliance and Policy • Internet and Network Security • Malware and Hardware Security • Wireless and Mobile Security

Comment on this article

Submit