DEALING WITH MOBILE DEVICES IN A CORPORATE ENVIRONMENT

RYAN WAKEHAM

September 2011

NETSPI™

BACKGROUND

Mobile computing technology is hardly a recent phenomenon but, with the influx of mobile devices such as smartphones and tablet computers into the workplace, the specter of malicious activity being initiated by or through these devices looms large. In truth, it is not the mobile devices themselves that represent the real threat; companies have had, and continue to have, good options available for controlling company-owned mobile assets and preventing other devices from accessing corporate resources. The paradigm shift that is occurring with mobile technology is really due to the convergence of corporate and personal use onto a single device.

A modern smartphone or tablet computer is not fundamentally any different from a PC in terms of either capabilities or threats posed by the device. Certain controls for mobile devices may still be immature or even nonexistent (e.g., anti-malware) and it is true that some of the risks cannot be mitigated as effectively on mobile platforms as on more established technologies. However, generally speaking, an information security toolkit that includes appropriate controls for addressing threats presented by corporate laptops should also be able to deal with company-owned smartphones.

The real complications arise when employees demand the ability to use corporate mobile devices for personal use or, alternatively, when personal devices are introduced into the corporate IT environment. A hardline stance against allowing this sort of activity is a good way to substantially reduce risk but, with managers and executives among the users wanting to consolidate their personal and company smartphones, such a stance likely won't last very long. Very quickly, information security professionals find themselves struggling to manage the risk posed by devices that are permitted to access corporate resources but that are not fully controlled by the company. These dual-function devices could be company-owned but have an assortment of downloaded personal applications or they could be personal devices connected to corporate wireless networks, email servers, web applications, and other data stores. Providing employees with mobile applications that allow direct access to sensitive data simply raises the stakes further.

While the challenge is certainly daunting, the situation is not as grim as it may seem. There are still strategies that can be applied to effectively reduce the risks posed by these dual-function mobile devices.

Very quickly, information security professionals find themselves struggling to manage the risk posed by devices that are permitted to access corporate resources but that are not fully controlled by the company.

EFFECTIVE STRATEGIES FOR MOBILE SECURITY

Establish a Strong Policy

Even if dual-function mobile devices are permitted, that doesn't mean that the company needs to throw in the towel regarding regulating them. Establishing a mobile device policy that outlines both the company's approach to mobile devices and employee responsibilities is the first step toward a more secure mobile environment. Once the parameters of acceptable use and required controls are established by the policy, additional supporting standards and procedures should be defined to enable the application of strong technical controls.

Educate Users

Security awareness training is a critical component of any good information security program. Mobile device security concepts should be integrated into current training material. In particular, make sure that users understand their responsibilities and how they can protect their devices, the data resident on those devices, and the corporate infrastructure to which the devices connect.

Implement Local Access Controls

While it should go without saying, mobile devices should be password protected just like other computer systems. If possible, this control should be enforced through technical means such as group policy; regardless of whether or not this is feasible, establish a policy requirement and educated users so that they enable the password protection features on their devices.

Minimize the Mobile Footprint

As noted previously, certain security controls do not exist for mobile devices like they do for more conventional computing platforms. Due to this fact, these devices may not be trusted to the same extent as assets that are fully controlled by the company and, as a result, present additional risk. Even if your employees have no bad intentions, one of their devices could become compromised and leveraged as an entry point into your environment. To combat this risk, treat the devices as semi-trusted: establish wireless networks specifically for such devices and implement access controls such as firewalls to provide access to only the minimal services necessary, as defined in the mobile device policy. If you only intend to provide corporate email and Internet services, ensure that your rulesets are denying all other traffic. Additionally, ensure that you have an intrusion detection/prevention system and network anti-virus deployed on this network segment to alert you if any sort of malicious activity is detected.

Restrict Connectivity

Consider the use of remote desktop functionality in the place of direct connectivity when allowing mobile device users to access sensitive data and applications. This will allow you to more closely track and monitor where data is located and prevent it from being downloaded and stored on mobile devices.

Restrict Web Application Functionality

Depending on what sort of corporate web applications you wish to be accessible to mobile device users, it may be beneficial to restrict content and functionality based on access mode. For example, if a particular application needs to be made accessible to mobile devices, it may be possible to classify functionality and content into that which should be accessible to mobile devices and that which should only be accessible to users on more conventional computer systems.

Assess Mobile Applications

Like any other application, an application running on a mobile platform is exposed to numerous threats, from interception of data in transit to compromise of locally-store data to plain old misuse. Mobile applications used to access sensitive corporate data should be assessed by application security experts for vulnerabilities in the file system, memory, network communications, and user interface.

Encrypt, Encrypt, Encrypt

The risk of lost or stolen data is not unique to dual-function devices or even to mobile devices; laptops and storage media can succumb to the same threat. Much as laptops and storage media should be encrypted, data resident on mobile devices should also be encrypted to the fullest extent possible. In particular, data in local mail stores and applications should be protected. Solutions currently exist for encrypting mail that is stored on the device. Applications, on the other hand, should be designed to encrypt any residual data that may be stored on the device. Additionally, protect data in transit to and from the mobile device. Using VPN, SSL, or similar technologies, you can encrypt communications channels and reduce the risk of data and credential compromise.

Enable Remote Wipe Functionality

Many devices support some level of functionality that allows a corporate administrator to remotely wipe data and settings from the device. Often, this requires the device to be connected to the Internet so that the kill command can be received. In some cases, though, dead man's switch functionality will automatically wipe the device under certain conditions, such as if the device has not connected to the corporate network for a certain amount of time. Enabling this functionality adds a layer of assurance that a lost or stolen mobile device will not result in a data breach.

Implement a Mobile Device Management System

There are a number of solutions available that have been designed to help manage mobile device security. Many of these enforce technical security settings on the devices, restrict access to certain applications or functionality, and protect certain data, such as corporate email and calendars, in a virtual sandbox. This sort of solution is not one-size-fits-all but it can be helpful by simplifying the application of controls across numerous mobile devices and platforms.

Provide Support for Employee-Owned Devices

Consider providing free help desk support to employees that have lost personal mobile devices, particularly if those devices had been used to access corporate systems and data. The help desk team should be trained on instructing users to change their passwords on work and non-work related systems and applications, as well as requesting a cellular service provider to remotely wipe or otherwise disable the device.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.
Follow us on LinkedIn, Twitter, and Facebook.