Securing Wireless Mobile Devices

Lamaris Davis

East Carolina University

11/15/2013

Attract

As more employees prefer to use mobile devices in the workplace, organizations are starting to adopt the Bring Your Own Device (BYOD) approach totally. This option leads to employees having more control over corporate information, and this is creating more work for organization's security team because they have less control over the mobile security. There are two most commonly used mobile operating systems being used today which are iOS and Android, iOS is produced by Apple and Android is produced by Google. It's very important to find creative ways to secure the wireless mobile devices that takes up so much of our time today. Most end users use basic rules such as setting a Personal Identification number (PIN) password or simply they choose to lock up their screen. A personal identification number is a secret numeric that can be used by a user on a system to authenticate themselves. Some end users chooses to utilize a security suite like Avast mobile security or Lookout Mobile security to protect their devices.

Mobile Devices

In today's competitive business environments, mobile devices such as smartphones and tables make up the biggest segment of computing devices available on the market-definitely growing faster than desktop and laptop computers, and that's according to a recent IBM study. As the demand of these wireless mobile devices grow in the workplace, more and more employers like Duke University Health System and IBM are adopting the Bring Your Own Device (BYOD) model-basically allowing employees to use their own mobile devices for business purposes. The adoption of the BYOD model leads to employees loading a bunch of corporate and personal applications on their personal devices, which gives the security department within an organization less control over what's on these various devices this was according to one of IBM's studies (2010).

As a direct result of the demand of wireless devices in the workplace, many organizations are starting to look more into the mobile security issue. Many organizations are starting to look at mobile security as a primary technology challenge for their organizations. The reason for the increase attention is because mobile security application environments have the ability now more than ever to access confidential or very sensitive information. Hackers have noticed the responsibility being put on mobile devices and have started to target mobile applications. These attacks have resulted in decrease trust among customers and especially the specific application environments. Even though some of these application environments have become mostly secure, there is definitely still room for improvement in the mobile security area.

Mobile Application Environment

For the smartphones and tablets in existence today the most commonly used application environments are iOS and Android. These two environments have the ability to be used with various applications. These range from web applications which run in the device's browser to native applications which incorporate one of the main applications available on mobile devices today.

Android is a mobile operating system produced by Google. Many different vendors produce smartphones and tablets that specifically run the Android operating system. The key benefit that Android have over iOS is the fact that Android is open source; so many manufacturers use the Android operating system because it can easily be customized to their liking. Android applications are available in an open marketplace called Google Play. Users can also download apps directly from websites to their mobile devices.

Mobile Application security compromised

End users are now able to install different types of applications on their mobile devices. Since most users have no ability to perform a security audit on the applications, the applications may be buggy or include some type of gap in the security of the mobile device. The applications do not have to be intentionally flawed, but some are most certainly flawed directly out of production. Most of these mobile devices are created with design flaws that directly make them insecure overall. Once an attacker gains access to your mobile device they can do a number of things like intercept internet traffic to sending well malicious data feeds to a user's mobile device, and it doesn't matter whether it's a tablet or smartphone. What most people do not realize is that mobile applications have the ability to access security-critical servers, storage database, and other major systems. If an attacker can exploit these applications some way they can

potential disrupt the systems or deface web-pages. The attackers could also gain access to address books, which leads to the attackers discovering personal contact information on different individuals. There were reports in the past that spoke about how Android applications could potentially lead to leaking of important information.

Securing wireless mobile devices

In a BYOD environment, mobile devices including smartphones and tablets enable employees' ease of access when working on assignments and to generally work from anywhere. With the BYOD environment comes the concern for the security of enterprise data, and especially on mobile devices in the workplace when there is a chance for them to be lost or stolen. The security rise is definitely lifted by the idea of employee-owned mobile devices in many organizations. Organizations that practice the BYOD policy are encouraged to clearly document and enforce a mobile security policy to reduce the risk of critical data mishanding.

When it comes to controlling access organizations must keep in mind that mobile devices are portable and can easily be lost. Some form of authentication, such as a personal identification number (pin), can make a mobile device more secure therefore making it more difficult for unauthorized users to access the device's information. There are solutions when it comes to the security of a mobile device. In addition to the standard numeric passwords, the user could also use some form of biometrics (such as fingerprints or face recognition), you could combine two or more security options to really secure a mobile device.

A recent study by the Ponemon Institute (2013) found the average organization cost of data breach increased to $1.2 Million and cost companies an average US $214 per compromised record, markedly higher when compared to $204 in 2009 and that's compared to 202 in 2008.

This information is real facts based off of a real breach if these things would happen worldwide, the annual total loss of revenue would be outstanding. These numbers show that companies and individuals have to prepare accordingly.

Battling a new wave of malware

The threat that exists for personal computer is huge, but the threat for mobile devices is just really coming on scene as of now. All smartphones should be treated like computers because users most of the time inadvertently infect their own devices by downloading a malicious app or by visiting a malware filled website. It's impossible for app owners to review code on all applications. To combat most of the problems seen recently by experts, they have started creating software security suites like the ones being utilized on most computers today (IBM, 2013. securing your end user device).

Setting the Policy

Today organizations are finding it hard to keep employees from bringing their own mobile devices to the workplace for business purposes. There are several things that IT professionals can do to get ahead of the security issue that will come up eventually. The first thing they could do is set policies and procedures to be followed regarding what data is allowed to be accessed on these mobile devices, how this information will be accessed exactly, and more importantly how organizations will directly deal with lost and stolen mobile devices.

Solutions

A mobile device management (MDM) solution could help with implementing a security policy for mobile devices in the workplace. Mobile security suite software may also protect

devices from malware and other bugs that affect mobile devices. These two combined together could provide a way for users to be notified in the case a security check failed, the user could be notified of these findings and take necessary steps to correct them. Citrix has created mobile device management software which is called XenMobile.

XenMobile allows IT departments to easily meet mobile security and general compliance requirements regarding bring your own device (BYOD) policies in the workplace. XenMobile provides the best solution when it comes to mobile user productivity. It's the best solution because it dramatically lowers the cost of ownership for an organization. It lowers cost because it gives users device and app choice while guaranteeing that they will still be in compliance. This software also provides advanced app and data controls to keep users pleased while guaranteeing content security for the IT department.

Conclusion

Mobile security will continue to create challenges for IT departments everywhere in the future. Even though security issues will make themselves known there are things IT managers can educate their employees and other co-workers on. They could simply suggest that they secure their mobile devices with Personal identification numbers when not in use. IT managers can also put a mobile device management solution in place like XenMobile software where mobile security can be closely monitored.

Mobile device security suites like Avast Mobile security or lookout mobile security can provide anyone outside of their workplaces with a reliable mobile security product. The free edition of lookout mobile security and Avast mobile security provides enough security for any mobile device you decide that need to have security installed. So with that said Mobile security

software will protect devices from malwares and viruses that roam the internet. When coupled with Mobile device management (MDM), the device's security position can be established before it connects to the network. If the device fails the security audit, the user can be notified and the device separated from others to reduce enterprise network risks.

Bibliography

IBM, 2008. Securing the mobile enterprise with IBM security solutions. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/wgs03003usen/WGS03003USEN.PDF on 11/05/2013.

IBM, 2010. Securing end-user mobile devices in the enterprise. Retrieved from http://www-05.ibm.com/innovation/de/engines/assets/securing_end_user_devices.pdf on 11/02/2013.

IBM, 2013. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html on 11/05/2013

Ponemon Institute, 2008. Data loss. Retrieved from http://www.ponemon.org/news-2/23 on 11/8/2013

Citrix. XenMobile. Retrieved from http://www.citrix.com/products/xenmobile/overview.html on 11/25/2013

PWC (2013). Managing security in a mobile workplace. Retrieved from http://www.pwc.com/us/en/it-risk-security/publications/managing-security-mobile-world.jhtml on 11/25/2013

Infosecurity-magazine (2012). Retrieved from http://www.infosecurity-magazine.com/view/23350/mobile-devices-in-the-workplace-cause-more-security-breaches-say-firms on 11/22/2013.

Ellis, Kathleen and Goldstein, Ken. Insurance Journal. Mobile Device Explosion in the Workplace Creates Need for Heightened Security. Retrieved from http://www.insurancejournal.com/news/national/2012/10/16/266765.htm on 11/23/2013.

Confident Technologies. Bring Your Own Device (BYOD) in the Workplace Demands New Authentication Technologies. Retrieved from http://confidenttechnologies.com/news_events/bring-your-own-device-byod-workplace-demands-new-authentication-technologies on 11/23/2013

Acohido, Byron. USA Today. Personal mobile devices create security headaches for biz.

Retrieved from http://usatoday30.usatoday.com/tech/products/2011-05-30-mobile-devices-in-

the-workplace_n.htm on 11/20/2013.