Audit Personal Phone

Student’s Name

Institutional Affiliation
Audit Personal Phone

Introduction

The concept of BYOD is a new global trend, hotly debated by professionals in the IT sector. BYOD abbreviation stands for “Bring Your Own Device” and describes the phenomenon of the spread of personal mobile devices in the business environment. It is also referred to as “consumerism”. Analysts believe that over time, this trend will take a global scale. According to research conducted by IDC, about 95% of the company’s employees are already using at least one personal device for work purposes. Estimated to Gartner, about 90% of companies plan to support business applications on devices owned by end users, as it will reduce hardware costs by 40% (Hayes & Kotwica, 2013). In addition, the popularity of mobile devices will help to “get in touch” with the employee even after working hours. For example, employees can view e-mails or work on a presentation in their spare time.

The concept of BYOD blurs the boundaries between work and private life. Nowadays, more and more employees are using social networks (Facebook, Twitter and Xing), in which professional and private contacts converge (Keyes, 2013).

These facts have confirmed the relevance of the issue of the business applications of smartphones and tablets in organizations and companies. It is not just a tribute to the fashionable gadgets, brought into the business environment of top managers, but the consequence of the real needs of organizations, including those related to the improvement of communications and existing business processes.

Mobile access is needed not only by leaders of organizations and units. The trend is clearly visible to the formation of categories of staff, called “mobile professionals”. This staff, which spends a significant part of work time outside their workplace, and, nevertheless, they need to be provided with a full-featured, timely and secure mobile access to corporate resources (Guerin, 2013).

It is clear that organizations pay attention not only to smartphones, but also to tablets. iOS and Android became the undisputed leaders among smartphone and tablet platforms. Therefore, if the iPad was recently de facto the only choice for corporate users, now there is a trend to increase in the share of Android-powered devices, which are considered to use nearly a half of organizations surveyed.

Variety of devices and platforms available in the market, in the context of the lack of updated corporate standards is the most common factor limiting the effective use of mobile devices. The second most important obstacle is the case when effective use of mobile devices in the corporate environment is limited by the information security.

Control over the use of mobile devices (MDM/EMM - Mobile Device Management/Enterprise Mobility Management) today is used only by 4-5% of medium and large organizations. The introduction of such funds can have a decisive impact on the legitimacy and ensure transparent control of mobile access to corporate information resources and systems within the policies and procedures adopted by the organization. More than 65% of IT managers are aware of the need for such solutions, so they will be considered and planned in the nearest future (Assing & Calé, 2013).

 Nowadays, with the development of IT consumerization, the attention of specialists is increasingly attracted by BYOD-technology. While some still prohibit the use of all non-corporate devices, many companies encourage the use of smartphones. At the same time, BYOD devices based on Android OS became a stumbling block for most IT-directors who are concerned about the possibility of losing control over information security.

Information Security Risk carried by BYODs in Enterprise

While adopting BYOD policy, the organization is often neglected in such analysis, resulting in a face both unknowns and risks with optional. In order for the company to
achieve success in the era of dominance of mobile devices in the workplace, risk
management should be the basis of its corporate policy BYOD. The use of personal devices
for storing and processing of confidential information is becoming more widely used in
business. This means that the organization is facing new threats related to theft, loss and
damage of data, malware and other attacks in the event that equipment is not protected and
security issues neglected.

Devices proprietary employees confront IT services with new challenges as
limitations on the use of corporate technology, they no longer apply. Among many aspects of
the information security of BYOD, the most threatening for the company is the situation
when employees inadvertently doing something inappropriate on personal devices they own
or those owned by the company. Given the fact that more than 200,000 versions of new
malware appear every day and the number of targeted attacks on the company grows, the
enterprises are in a very dangerous situation (Harkins, 2013). At the same time, most
companies do not plan (or are not able) to complete block the access of personal devices to
corporate data. For a deeper understanding of the risks of BYOD policy, it is imperative to
review traditional computers, smartphones and tablets separately.

Laptops

Malware

It is quite obvious that all computers with access to the corporate network must be
protected against common threats, such as malware. It is important that methods of protection
should be the same for both corporate and personal devices. Different security solutions for
different network nodes are the most likely to cause problems. Even the antivirus protection
preinstalled on a laptop brought by a user does not solve the problem. All devices such as
company-owned and private ones should be provided with a single type of corporate security
and managed centrally. This will help to eliminate the most common cases, when a weakly
protected personal computer infects the entire corporate network. The alleged offender is
usually difficult to track when devices are beyond the control of the network administrator.

Dangerous Legal Software

If the preceding paragraph was relating to programs of the “black list”, deliberately
malicious, this one applies to the “white list”, or legal software. The software must be under
the control of the IT department to minimize the security risk. In a typical corporate
environment, it is achieved by limiting the ability of employees to install additional software
on the computers. However, in the case of personal laptops, it is not always possible. Instead,
installation and usage of the software must conform to strict rules under which each program
is classified according to several criteria. This strategy helps to avoid cases where an
employee sends all corporate documents to a personal cloud storage service, which, in turn,
due to a possible burglary puts confidential information at risk (Vacca, 2013).

Targeted Attacks

Personal devices may be the most vulnerable to targeted attacks using methods like
fishing, when an attacker sends to employee a specially crafted email offering to open an
attachment that uses vulnerability in a certain program. To effectively address this threat, a
number of criteria must be fulfilled:

- Modern full-featured anti-virus protection is required;
- An effective web antivirus to detect and block dangerous web pages is necessary, as
well as limiting access to certain web resources, such as online games, during working hours,
which will also help increased productivity;
- It is necessary to monitor the installed and used software, which will see to the
application vulnerabilities. Regular updates for critical vulnerabilities in software should be a
part of corporate security policies.
Loss and Theft of Devices

Typical nightmare for the IT department is unprotected and the information stored on a personal laptop that might be lost at the airport or in a taxi. Some companies solve this problem by allowing employees to work only on office computers with very limited data transmission capabilities and disabled USB-ports for flash drives (Vacca, 2013). This approach, in fact, will not work in BYOD oriented company. First of all, the employees use their computers for more flexibility, but it should not have any impact on the level of security. The ideal solution to the problem of a lost device is full or partial encryption of corporate data provided by company policy. Then, even in the case of theft of a laptop or a USB flash drive will not be able to access the data on them without a password.

Smartphones and Tablets

The number of threats to mobile devices is less than that for traditional computers; however, it is growing rapidly. In fact, in 2012, over 3,000 new malicious programs for Android appeared every month. The situation with Apple IOS devices differs from carefully controlled software environment that currently eliminates the threat of malicious software for this platform (except the cases when malicious programs appear in the official App Store). However, this does not mean that iPhone and iPad are the best choice for BYOD concept from a security standpoint. All devices are at risk of data loss due to theft and/or improper use of legal software such as cloud services (Harkins, 2013).

With this in mind, the problems of a general type of malware, dangerous legal software and loss of devices, in the case of traditional laptops, apply to mobile devices too. Particularly relevant in this case is the problem of lost or stolen devices. In fact, smartphone protection from thieves is as important as protecting it from malware. Fortunately, at the moment, targeted attacks on smartphones are unlikely. Since cybercriminals are not yet ready to exploit vulnerabilities in the Android or IOS for data theft. However, Android-powered devices are already being targeted with the use of social networks and malware. There are several unique features in regard to threats to mobile devices within the concept of BYOD (Harkins, 2013).

Rooting and Hacking of Devices

Rooted Android smartphones or cracked iPhone or iPads are, in fact, beyond the safety control: the owner of the device can install, remove or modify any program or even a part of the operating system code. Mostly, it means that all the controls and protection company can be circumvented by having access to corporate data. In the case of malware infection, the malicious application will also receive full access to all functions and data of the device. Thus, the rooted device should not have access to confidential data (Vacca, 2013).

Enhanced Protection against Theft

As mobile devices are easier to steal and lose, it is important to use additional ways to protect the data stored on them. The first method is the same for all devices - the encryption. All corporate data should be encrypted to make it inaccessible for thieves or spies. The second method provides the ability to remotely lock or clean a smartphone from all the data stored in it in case of theft or loss. Employee is required to notify the company’s IT department about the loss of the device, after which a special team will be sent to lock a smartphone or remove from it all important data. They must also be able to determine the location of a lost device and do not forget that on different platforms the implementation of antitheft function differs.

Inherent Security Vulnerabilities in Android

Android OS has become one of the most popular systems for all kinds of mobile devices. It is used both by the major manufacturers with a worldwide reputation and small companies, so price spread of products, such as smartphones and tablets, fully meets the
needs of consumers. Its wide range, flexible pricing and support from the impressive number of manufacturers have become one of its main success factors and allowed the system to take the current place on the market.

Like any other system, Android, unfortunately, cannot be completely safe, as people involved in the design, will never be able to create the perfect code. Nevertheless, the developers put the effort in order to give a quality product to the customers. Android is a vivid example of a statement that the more popular the product, the more it is prone to malicious attacks.

Android architecture is designed so that all applications work with limited rights and do not have access to protected data from other applications.

As was mentioned above, Android is not a perfect system. One of the main problems that users might encounter is the vulnerability of the system, which allows getting root rights. There are special applications, scripts and software modules that perform this task. They are often used deliberately by users to gain more control over the device. Another thing is that the same vulnerability (e.g., CVE-2009-1185, CVE-2011-1823) has been adopted by the creators of malicious applications (Misra & Dubey, 2013). Using exploits (the same software modules and scripts) to improve their rights to the level of root, they are able to easily install other programs without the user’s permission (as do various modifications). Some malware do not use exploits directly, but misleads the user and encourages him to perform the necessary actions.

One of the key elements of the security system is Android Permission System. When users install the application, it shows a list of all the functions that will be available to program. After installing the application, it is able to perform the functions inherent in it without user’s intervention. On the one hand, demonstration of the possibilities before installing programs should provide an appropriate level of security, but not all users carefully study the list of functions. Moreover, it cannot be said with certainty whether one or another function would be used to the detriment of the user. Still, it is not the last drawback of this system. For example, it is possible to create applications that will not require any permits for their work, creating a false sense of complete safety. But in fact, these applications will be able to access certain information (for example, files stored on a memory card in an unprotected form, the list of installed programs used by the mobile operator) and even send this information via the Internet to attackers (Misra & Dubey, 2013).

The use of informal or third-party firmware can also pose a threat. There are a few causes for concern. Firstly, such firmware can be initially inserted with malware. Second, when a digital signature system image is signed by any application, it gets the same rights as the system in which it operates. Within the Android Open Source Project (AOSP) signature for the images are private, so this scenario is possible, for example, in the case of theft of the signature. Such a method of infection is used, in particular, by Android/J.SMSHider.A. Malware, which could, without being detected by users using certain third-party firmware, install the apk containing Trojan (Hoog, 2011).

System applications, both standard and applications from vendors of Android-devices are also a subject to vulnerabilities. For example, vulnerability of WebKit browser allows potential malware to execute arbitrary JavaScript code and gain access to protected data of the browser (Misra & Dubey, 2013).

If the application software developers do not pay sufficient attention to safety when working with data users, this data can be compromised. The data stored in an unprotected form, such as registration data, passwords of bank cards and other confidential information may be subjects to attack. In the case when during the work of application the same data is sent over the network unencrypted directly, it is also potentially subject to compromise by intruders. One notable precedents of such problem was the situation with the application...
Skype, when data of users, including profile information, contacts and correspondence history was stored in an unencrypted form and could be easily obtained by hackers (Hoog, 2011).

The openness of the Android system has a number of factors. First, the availability of a code which may be used, modified, and improved by the developers based on their needs and ideas. On the one hand, this is a definite plus for device manufacturers and application developers, on the other hand, it gives the opportunity not only to developers, but also to attackers to find vulnerabilities and bugs.

Secondly, there is the possibility to install applications as from the application directory of official Google Play (previously called Android Market), and from any other available source.

Third, the creation of applications is practically accessible, since it is necessary to pay only $25 fee if the developer wants to place his products in the catalog, and for the dissemination of programs outside material costs are not necessary at all (Hoog, 2011).

Fourth, applications placed in Google Play were not subjected to pre-screening or testing by Google until recently. However, the system called Bouncer was announced, which must check the applications for malicious functions; the accounts of developers also will be subject to verification. Of course, this will increase the safety to some extent, but it still does not solve the problem, as malware developers can use various tricks to successfully bypass Bouncer system (Misra & Dubey, 2013).

Because the system is used by a large number of Android mobile device manufacturers, and thus there is no specific framework for their technical characteristics, the devices are available to consumers with very different functionality. The release of the next system update adds not only new features, but also closes the previously discovered vulnerabilities. Manufacturers issue the appropriate version updates at their discretion. Sometimes the device being the former flagship will not receive a new version of the operating system or software and, accordingly, will remain unprotected from potential threats. The reason for this can be both economic considerations (adaptation updates require too large financial investments, or the manufacturer simply wants to make money on sales of new devices) and purely technical (the update will not work correctly on older hardware).

Whatever is the level of security of the system, the human factor plays the vital role in it. Very often, the elements of social engineering techniques are used by hackers, for example, previously mentioned method of distributing malware through advertising in applications using loud phrases (“System upgrade is required”, “Your browser version is outdated”, “Update Skype immediately”, etc.). The same can be said about the case of distribution of malware using spam through SMS (in this way, for example, the backdoor Android.Crusewind was spread) (Misra & Dubey, 2013).

In addition, the attentiveness of users is very important. Quite often the attackers spoof known sites, mimic their design, structure, or try to create an exact copy. At first glance, such a site may look exactly like the real one, but on closer inspection it is possible to notice the trick. For example, the address bar will be completely different from the original, or have a little distortion (e.g., androldmarket.com), or any habitual element will not work, or something familiar will be missing at all (Misra & Dubey, 2013).
References


Guerin, L. (2013). Smart policies for workplace technology: Email, blogs, cell phones & more. Nolo.com


