Mobile Device Security

[1] Amanda Zeqiri
Department of Applied Mathematics
Faculty of Natural Science, University of Tirana, Albania
Tirana, Albania
amanda.zeqiri@fshn.edu.al

[2] Igli Tafa
Department of Information Engineering
FIT, Polytechnic University of Tirana
Tirana, Albania
itafaj@fti.edu.al

[3] Redisi Mali
FIT, Polytechnic University of Tirana
Tirana, Albania

[4] Jon Shkreli
FIT, Polytechnic University of Tirana
Tirana, Albania

***Abstract*— Mobile devices are a big part of our daily life, and an integrated part of the daily business processes, due to the advantages that these devices offer. Businesses use these devices to gain a competitive advantage in the market. But this request for the mobile device to be added to the assets of the organization, comes with a price, and that is security.**

The mobile device user and the organization need to understand that this approach toward the access through mobile devices of the organization's data and sources it is a big security matter. As the data that the mobile user will access in the remote device or his own mobile device is at risk. With risk, we understand the risk that comes with the network, applications, data loss, out-of-date devices/apps etc.

Keywords: Mobile device; malware; cyber security; data loss; applications; BYOD; smartphones; data loss.

I. INTRODUCTION

Mobile devices are already an integral part of every business process. That's because they offer more flexibility, improved communications between employees and customers, more efficiency and productivity, in the same time keeping organizations competitive. Devices are just like offices in hand. Every time, whether commuting, travelling, sitting at home or working in the fields. Many organizations allow their employees to use the same devices for both private and work purposes. The phenomenon called Bring Your Own Device (BYOD), is when employees use their devices to complete work tasks, is an example of that. It was at first very popular but now the trend has turned and the popularity of BYOD is decreasing (Kane, Koetzle, Voce, & Caputo, 2014). Even though BYOD is decreasing, the question of how mobile devices should be handled, regardless of owner, is still relevant. Despite that the mobile device is owned by the company, it can be assumed that the user may choose to use it for private purposes also, so it becomes a dual-use device.

All these complex organisational environments require higher awareness from both employees and the organisation about information security implications. Also, they set higher demands for the organisation's information security functions and information architecture. While owner can access information easy, this too increases the risk that it may go into the wrong hands. Then attacks on mobile devices.

"The problem is that around 28% of CIO-s have declared that their organisation doesn't even have a mobile strategy, which means that they don't relate the usage of the mobile devices inside their corporation with their business objectives, 36 per cent say that they do not provide mobile security training for employees and another 31 per cent provide security training, but not on a regular basis. "(Samsung, 2016). There might have been cases when an attack, such as a data theft has happened and the damage in financial and public relations has not been significant. This makes them harder to chase and put them in low priority tasks. Meanwhile impact can be much bigger in the future once the vulnerabilities are exposed. Mobile development is growing rapidly and threads are becoming more advanced. Detecting and remediating them needs be a priority by each company.

II. RISKS THE BUSINESS FACE IN MOBILE DEVICE USAGE

Mobile devices nowadays are so popular and fuzzed with everyday live and activities. The businesses have adopted such a culture as their own, and have interlaced this culture with the way that they do business. The services that mobile devices offer to small and medium enterprises (SME) are helpful for the business. Such services help SME employees enhance productivity at a lower cost. This way technology is cheaper and benefits mostly small businesses.

Even with is great services mobile device usage comes with threats for the security and safety of the information that the business holds, its and the customers. These threats are greater id the business is so small that it does not have the finances to support the security infrastructure.

Some of the threats are going to be explained below.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

A. *Malware*

This is not a new term in the field of information security but sure is in mobile security. With the increase of mobile apps came even the raise of malware dedicated to these mobile devices. Based on a survey conducted by the University of Carolina, USA in 2012, malwares in Android system are at a way higher than iOS. These malwares come in all shapes and sizes. Some of them are:

- Fake applications

These applications try to look and do functions of real app. These applications execute malicious actions, like displaying ads aggressively so that they can rake in ad revenue or they can harvest information, like credentials, or access sensitive date. These fake applications can easily access by Android users, as for iOS users it is more difficult.

- SNARF attack

SNARF attack is when a large file of data it is being accessed and used without the owner's permission.

- Premium SMS

Aa malicious code that use standard Android API's to send SMS from a device. This SMS are sent to premium numbers that is costly. All this is done without the owner's knowledge and this is and can be costly.

- Zitmo and FakeToken

This type of attack it is distributed through phishing as the third party pretends to be a bank authority. PlaceRaider

The "visual malware", as it is called differently uses the mobile device camera to gain photos of the indoor environment, and recreate a 3D model of it. The phone does not give signs that the camera it is being used and the images captured are send directly to a server and not stored on the device.

- Backdoor attack

TimpDoor, an Android malware family that does backdoor attack. It has first appeared in March 2018, it quickly became the leading mobile backdoor family, as it runs a SMiShing campaign that tricks users to downloading fake voice-messaging apps.

These virtual backdoors are now a big threat and growing as third parties that are interested has begun to take advantage of the always-connected nature of mobile phones and other connected devices. Once distributed as Trojanized apps through apps stores, like Google Play, these backdoors can come disguised as add-on games or customization tools.

- Bluebugging

is a form of Bluetooth attack often caused by a lack of awareness. One that it is successful it can create a backdoor and gain control over the device. The unauthorized party can then make calls or even listen to the calls that the owner has.

- Out-of-date devices
- Cryptojacking attacks

Is a form of attack where someone uses another device to mine cryptocurrencies without permission?

- Data theft

Data theft is one of the most serious issues when talking about security. Nowadays everything is mobile oriented and users tend to download data on their mobile devices for a more comfortable usage and they keep this data in their mobile device as they fear of the connectivity to the business database in any time that they like.

As said above, even the loss of the mobile device can result in information leakage and loss of significant data. The theft it is much worse than just losing the mobile device.

Data loss can damage the business reputation, legal issues and costs for losing customer data, and based on the country that the business operates and the location of the targeted customers in legal fees for failing to protect the data.

B. *Mobile device OS and their Market policies*

In this topic, we are going to talk about the giants of the OS for the mobile devices, Android and Apple iOS. The security model that iOS uses is much safer that the model of security of Android. This I because iOS forces its users to download apps only from one place. While, Android users can download apps from every source possible. Also, equipment comes from various vendors by many carriers.

This is one of the biggest differences between the two giants of the OS for mobile, restriction vs freedom, but both have advantages and disadvantages.

In iOS process is very strict, both for developers and applications. This way security is higher but the disadvantage is that it takes more time to publish an application. Also all applications can be published via App Store which is Apple's applications market. On the other side Google gives more opportunity. Developers can publish applications through official Google's Play Store or in other third-party markets. This leads to high vulnerability.

iOS biggest advantage compared to Android is security. Apple App Store, limiting carriers, and single product creator, leads to higher security. On the other side, this create the big drawback for iOS. Customers want to choose in carriers, configure their devices, and download apps from many markets. This pushed customers towards jailbreaking which is major risk.

C. *What is Jailbreaking and rooting*

Jailbreaking it is associated with Apple devices. This term it is referred to a process which removes the platform restrictions. After these restrictions are removed the users have admin control and can install application from different markets.

"Jailbreaking and rooting makes device more vulnerable by giving easy access to malicious software [9]. These restrictions which are broken by jailbreak/rooting has been made for a reason. Also, both companies Google and Apple does not support this process.

The concerns for corporations are high because of their security threads. These jailbroken devices provide high

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

security threads because of the nature of jailbreak. The rise of these concerns has led to banning jailbroken and rooted devices from organizations network. [9].

D. Connectivity – WiFi

As mobile devices are all the time connected to the network the users should be aware not only about the security of the device but also about the security of the network that these devices are connected.
Elcomsoft's Wireless Security Auditor was released, in 2010. By brute force, it could break 103,000 WPA2 personal mode (PSK) passwords per second [9]. Some experts even recommend using wired connection instead of the vulnerable WI-FI [9].

III. MOBILE ATTACKS MAIN REASONS

There are six significant reasons attacks are made:

1. **Large attack area** – With such a growing market of mobile devices now is opened a gate for hackers to get information.

2. **Not protected technology** – usually devices are unprotected.

3. **Access to corporate networks** – Data from corporate and private life makes it target for hackers.

4. **Financial rewards**

5. **Risky user behavior** –Sharing data with unknown devices in public WI-FI, downloading unverified things, clicking suspicious links.

6. **Hybrid device for business and personal use** – Employees use their device to access company information and company device to access private information.

IV. INTRODUCING CONTROL PROCESSES FOR MOBILE DEVICE ACCEPTABLE USAGE

The IBM Security uses a closed-loop risk-management based framework for managing security that is adapted to specific security controls. This framework follows a basic plan and do and check and act/react set of components that IBM adapts to IT security management as:

- Security Policy Management
- Control deployment and execution
- Risk and Compliance Assessment
- Command and Control Management

Security Policy Management is not discussed in this article as its content is very long.

A. Control Deployment and Execution

To manage and ensure security of mobile devices like smart phones and tablets, a software or hardware is used which is called Mobile device management (MDM). In here are included not only BYOD devices but also those issued directly from the company. MDMs are capable of not only being integrated to the current system, but also managing devices of different platforms such as Android and iOS. This always more freedom to the employee to choose whatever hardware he prefers and not being limited to a narrow and soon to be outdated list of applicable devices. However, depending on the required features the cost of this system may vary greatly and it's not a viable option for all companies.

B. Android

For the android platform MDM systems offer these features for the following situations. Similar approach can be done for IOS, but it is not discussed in this article.

- Anti-theft

Measures against theft can be triggered either manually or automatically. The MDM can be configured such as when the SIM card is changed without prior notice, measures are executed automatically. On the other hand, commands can be sent through SMS. When a mobile device has been stolen or lost, the most effective way to send a command is via SMS messages to it. Administrators have quite a few available commands such as:

- Send an e-mail with location data of the mobile device to the administrator.
- Reset device to factory defaults. Meaning all personal data will be erased.
- Trigger alarm sound. This can help when the device is lost and stuck in a place where it's difficult to be noticed.
- Mute all ringtones, except the one triggered by the alarm sound option.
- Enable lock screen by using the password.
- Make screen password to a more difficult and harder to crack password, known only to the administrator. [10]

But there are cases in which the SIM card is immediately removed after getting stolen, making it impossible to send SMS messages to the mobile device. As a way to counter it, you have to predefine actions for such cases. The phone can be either locked and it displays a message to contact the administrators if you want to unlock it. Either way, these kinds of measures heavily affect the usability of the phone by restricting the user. For this reason, it is recommended to inform the

- Applications

MDM systems offer quite a few features for app management. First, you can scan for all the applications installed in the mobile device and get all the information about them such as name, version, size. For each app the administrator can get information about the vendor, it's version history though the official app store or by looking it up to the vendor's homepage. After analyzing all this information, the administrator can then decide which app to put in the whitelist or blacklist. In this manner all the applications deemed

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

unsecure or as a threat to the company's system can be blocked from running.

- Real-time and on demand protection

While using browser, protection in web is available. This protection is real time. It protects from malware and block the installation of apps other than from the official apps store. It can also be configured so that the mobile device can connect only to specific Wi-Fi networks.

- Contact management and filtering

Depending on the use case of the employees, it might be a better choice to use the corporate phone book to manage contacts on Android devices. To ensure control over the contact information the administrator can block the built-in device phone book and populate the corporate phone book instead. In addition, with call filtering, it can offer extensive contact management and filtering possibilities.

C. Mobile Devices Risk assessment

For mobile device risk, assessments the organizations can follow steps below:

1. Asset Impact

- To evaluate an asset impact first we consider a mobile phone's value like a ***device***.

- We should also evaluate mobile devices in the terms of the ***data*** they hold. This data might be at various types like: Personal data, Business data, Government, Financial data, Authentication data (user credentials like passwords, biometrics). For each data-type user should judge: "The worst consequences if that data is unavailable?", "The worst consequences if that data is disclosed to the public?" etc. The answers will calculate terms of unavailability, modification and disclosure.

- ***Network*** impact: for example, "Which are the consequences if your Wi-Fi is been observed?", etc.

- ***Applications*** impact, where the same procedure of evaluation is used.

- ***Total impact*** valuation. using data from above user can predict the impact of consequences (loss of availability, confidentiality and integrity).

2. As the second step we evaluate the threats where each threat is grouped and mapped with the security attribute that it impairs. For example, consider the table below:

Table 1. Smartphone threats (Theoharidou1, Mylonas1, Gritzalis, 2012)

Dimension	Threat	C	I	A
Network Connectivity	T1 Spoofing	✓	✓	✓
	T2 Scanning	✓		
	T3 Denial of Service, Network congestion			✓
	T4 Spam, Advertisements			✓
	T5 Eavesdropping	✓		
	T6 Jamming			✓
Device	T7 Loss, theft, disposal or damage	✓	✓	✓
	T8 Cloning SIM card	✓	✓	
	T9 Technical failure of device		✓	✓
Operating System	T10 Unauthorized device (physical) access	✓	✓	✓
	T11 Unauthorized Access	✓	✓	✓
	T12 Offline tampering	✓	✓	✓
	T13 Crashing			✓
Applications	T14 Misuse of Phone Identifiers	✓		
	T15 Electronic tracking/surveillance/exposure of physical location	✓		
	T16 Resource abuse			✓
	T17 Sensitive Information Disclosure (SID), Spyware	✓		
	T18 Corrupting or modifying private content		✓	✓
	T19 Disabling applications or the device			✓
	T20 Client Side Injection/ Malware	✓	✓	✓
	T21 Direct billing		✓	
	T22 Phishing	✓	✓	

3. Risk assessment. As the risk evaluation we can create a vector for each asset where we determine the asset impact and the threat likelihood related to that asset. This helps the organization to be more aware in specific assets with higher risk.

4. Document final risk determination

5. Establish underway monitoring of risks and response.

D. Control Management

Control management on the mobile device usage helps monitoring and assuring that everything is working according to the policy we've implemented.

- **Control effectiveness assessment process**

To measure the effectiveness of controls, the organization gets some performance metric reports which show what process has worked properly and which not. If a part of the IT infrastructure cannot manage mobile device controlling, company should improve that or accept the risk.

- **Outcomes assessment process**

Tis process checks statistics of incidents and data thefts and determines how the policy of mobile devices control has affected.
Below, we take an example of some of the issues and controls applied to an organization.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Issue	*Control*
Employees responsibilities	-The organisation employees must immediately report the loss or theft of any mobile to the IT Department. -Employees who use their personal device to access firm email must immediately notify the IT Department of any loss or theft of their personal device so that proper security countermeasures can be performed.
Remote connectivity	- The IT Department is authorized to erase, destroy or reset any data stored on any mobile device, like tablet or smartphone to ensure the safety and privacy of any data related to the organisation and contained within the device. - Any mobile device that is connected to the organisation's network shall have the password protect feature enabled. - The IT Department may install 3rd party software on any mobile device used within the organisation to assist with their management and protection.
The mobile usage	-Mobile devices used by employees accessing its network are on their full responsibility. -Employees cannot use the organisations devices to access their personal data or email, social networks etc. and if they do, they should be aware they're giving up on their privacy - Any data that is created, stored or sent on the mobile device which is the private property of the organisation shall be treated as such.
Management responsibility	- All mobile devices must be registered to a named individual who is responsible for ensuring the security and correct usage of that device. - Managers should instruct their staff to a safe usage and security of devices in their possession. - Managers are responsible the staff training in all aspects of their work that includes use of mobile devices and all computer equipment, assuring that they only use systems for their intended purpose.
Device management	- All mobile devices will be connected to a central management system to ensure security and system integrity of that device. - Devices will be secured through encryption, anti-virus, and configuration management systems. - Devices which are shared by multiple users require individual unique login credentials.
Applications	- The IT department will maintain a central store of approved applications and software. - Staff can only be able to download any licensed applications allowed from the IT department to the tablet or smartphone device.
Lost Devices	-Lost or stolen devices must be reported immediately to the IT Department where disciplinary actions may need to be taken.

V. CONCLUSIONS

The rapid growth of mobile devices and BYOD are putting pressure in IT organizations. A group of new threads is appearing to company data, cyber-attacks and privacy loss. Even thought, there is a possible approach to increase mobile security and why not improve company security generally.

In today world we are seeing more and more where IT departments store company data and applications living on mobile devices and can monitor activity, detect threats and respond.

This is a new approach that makes BYOD effective by offering the balance between user satisfaction, employee productivity, security of corporate data and IT compliance. IT organizations can go a strategy where they manage risk of mobile devices. This can be done via layered security, thread assessment, policy management and integrity verification.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCE

[1] "Understanding the mobile threat landscape in 2018", Wandera, 2018

[2] "The mobile security evolution", Samsung, 2016

[3] "A risk assessment method for smartphones", Theoharidou1, Mylonas1, Gritzalis, 2012.

[4] "Sample Mobile Device Management Policy", Brophy, 2015

[5] "Mobile Device Management (MDM) Platform Buying Guide." Rubens, P., 2012.

[6] "Achieving Rapid Payback with Mobile Device Management" O. R., 2012

[7] "Rhee, K., Jeon, W. & Won, D., 2012. Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications," 6(2), pp. 353-358.

[8] Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, Pages 3-14

[9] A. Harris, M. and P. Patten, K. (2014), "Mobile device security considerations for small- and medium-sized enterprise business mobility", Information Management & Computer Security, Vol. 22 No. 1, pp. 97-114.

[10] Mobile Device Management, G DATA CyberDefense AG | September 2019, https://www.gdatasoftware.co.uk/fileadmin/web/en/documents/techpaper/G_DATA_TechPaper_Mobile_Device_Management_English.pdf "Understanding the mobile threat landscape in 2018", Wandera, 2018

https://sites.google.com/site/ijcsis/
ISSN 1947-5500