"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

BYOD IN LARGE ORGANIZATIONS

Vlad Mihai COTENESCU[1]
Cristian-Gabriel APOSTOL[2]
[1] Eng., Electronics and Telecommunications Faculty, Doctoral School, Military Technical Academy
[2] Eng., Electronics and Telecommunications Faculty, Doctoral School, Military Technical Academy

Abstract: *The Bring your own Device concept started to be increasingly adopted by companies and institutions as they try to provide extended mobility to their employees or students without decreasing their quality of work. One of the other significant advantages that this concept introduces is the cost saving part in respect to device purchasing, management and maintenance. Furthermore, because employees are more familiar with their own device the number of support calls should decrease and, with employee awareness programs, patching and updates will fall under their responsibility. Driven also by the growth of the number of mobile platforms available BYOD has the intent to provide customers and students ease of access to the organization's applications. Accessing information in real time irrespective of the location or time offers the potential to increase productivity. Having your entire workplace accessible through a thin client (app) on your phone or tablet would give you the opportunity to deliver your work using only an internet connection. In the same time BYOD introduces a series of concerns as now the perimeter of the network, becoming so volatile, would be harder to secure. Having personal devices accessing the internal assets of the organization from anywhere leaves doors open to unauthorized access, malware attacks or information leakage. In the end in order for organizations to adopt and implement BYOD, there has to be a compelling business case to support it and the rewards must outweigh the risks.*

Introduction

More and more public institutions and companies are giving the opportunity to end users or employees to access intranet resources using their own mobile devices. This movement, called BYOD (bring your own device)has a significant impact on the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership; for the organization alongside the benefit of cost savings comes the increased risk of security exposure and for the end user there are privacy concerns for their data. Recent studies suggest that in about five years, the number of mobile devices will be about10 billion — 1.5 for every man, woman and child on the planet.When it comes to our personal lives we can see that we start becoming more and more dependent on these mobile devices for conducting work, interacting with others, keeping track of our daily activities or doing or daily groceries. As a company is very difficult to stop an employee to use his corporate device for doing both work and personal agendas, but you need to have the ability to control it. In the current economic environment, companies are pushing employees to be moreproductive and look to have personal devices to be used for accessing corporateemail, calendars, applications and data; This article, has the purpose to present the main risks of BYOD when considering yourmobile device program, and we will propose potential steps to address these risks based onyour organization's current and most urgent challenges.

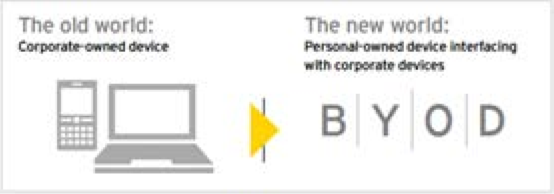

fig. 1

Hypothesis:

When you are deploying BYOD in your environment you should take in consideration that the risk landscape of mobile devices is highly dependent on a few key factors. One of the things to consider when moving to a mobile workforce that isn't managed centrally is the geographical distribution of the devices. Some areas, like the European Union have stricter legislation when it comes to privacy and personal data. Another aspect, related to privacy, that needs considering is current and future data use cases. Some companies might not want to have SSN's, financial account numbers, passport numbers or credit card data stored of processed using mobile devices. In case companies decide to allow credit card processing on personal devices they would require to be compliant with the PCI-DSS standard. According to current research, here are a few challenges that were identified:

- Mobile device security
- Data breach security
- Mobile data security
- Mobile application security
- Integration with back-end corporate systems
- Controlling employee use of mobile apps
- Cost of help desk support
- Country-specific regulations
- Executive sponsorship
- Expense of implementing applications
- Industry-specific regulatory requirements
- ROI of BYOD
- Cost of training
- Mobile app development costs

Since all the mobile workforce won't be managed by the internal IT department the organization is not opening herself to the risk of having an increase in the effort invested in keeping an accurate and up to date asset inventory. In the same time the It departments would face the task of keeping the operating systems of those mobile devices up to date and having to support an increasing number of device types.

In the mobile device space the turnover and evolution is significantly more rapid than in the traditional PC asset inventory. In such a rapid growing environment system updates are frequent and often need to go through layers of validation and customization before being applied to an end device. For example, for Android devices the OS updates are reviewed at three different levels before the end user can install them; OEM vendors use software customization to verify that update doesn't impact user experience, manufactures test to make sure the update doesn't impact their hardware functionality and cellular carriers often hold back on updates until they are sure that connectivity is not impacted. After all necessary checks are completed and the updates are released to the general public it often happens that the updates are not obvious or installation is not mandatory. In this case performing actual software upgrades is at the discretion of the end user which would need to be properly educated in order keep their mobile device up to date. To sustain this education the organization might need to create a patch education process and setup an internal knowledge base support solution.

As end users rely now solely on their devices to access the organization's resources and application that might introduce incompatibility issues which might be overpassed by introducing minimum hardware and software requirements for all accepted devices. These minim requirements might also address some security concerns related to encryption; for example, some iPhone models lack hardware encryption. Some costs related to the data plans or costs of acquiring the device might need to be supported by the organization.

Raising awareness of these challenges will help organizationsand their employees understand the critical areas which can helpsecure their mobile devices, thereby promoting enhanced informationsecurity. Risks relating to securing mobile devices are categorized into five basic concerns:

- Lost and stolen devices
- Physical access
- The role of end user device ownership
- Always on with increased data access
- Lack of awareness

In order to manage all these shortcomings, organizations need to adopt a MDM solution that will allow users to recover, wipe or block data in case of the device is stolen or lost. In the same time the organization would be able to push to devices different policies that can control application utilization or enforce acceptable data use.Another important piece is enabling security features as password protection, encryption and robust procedures to wipe de device. All these features are important since the threat model is different than for hardware such as workstations or servers, where physical access is less likely or other compensating controls are in place. It's a lot harder to properly secure a device once an attacker has gained physical access.

End users utilize their mobile device to access and store work related and personal data. This behavior can't be stopped and organization should start learning to embrace it and focus on addressing the introduced risk. The sense of ownership might make users have the impression that they are entitled to unlock, "jailbreak" or "root" the operating systems of the mobile device; by doing this they might turn off or remove many security features and in the process introduce new vulnerabilities. Periodic auditing should be performed on the status or the integrity of the operating system of all devices.

Although having an MDM solution offers the organization a way to manage risk, the wide diversity of mobile device types might result in having the security controls not applied consistently and effectively across the mobile device population. In addition, operating systems or applications introduce vulnerabilities that can circumvent these controls. With an MDM solution can provision certificates down to the device and have security controls enabled such as: screen lock, remote wipe, encryption and so forth.

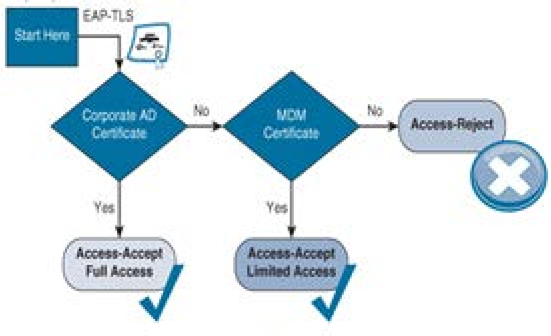

fig. 2

One of the greatest advantages of BYOD is that end user get the ability to be always connected. In previous scenarios employees left most of the data at the workplace but now they are travelling all over the world and they are in constant need to access the organization's resources.

This behavior maximizes the risk of having a data breach or loss. Thenumber of Wi-Fi hotspots has grown exponentially, exposing more mobiledevices to hackers who monitor traffic on open networks. In addition, losinga tiny smartphone is easy to do. McAfee, the security company, saysthat over 4% of smartphones are lost or stolen each year. Each unsecuredstolen or lost phone opens the organization up to the chance of a breach ofcorporate systems and/or data. [4]

Utilizing a mobile device an attacker could leverage VPN connections or security bugs in personal apps to gain access to the internal assets of the organization.

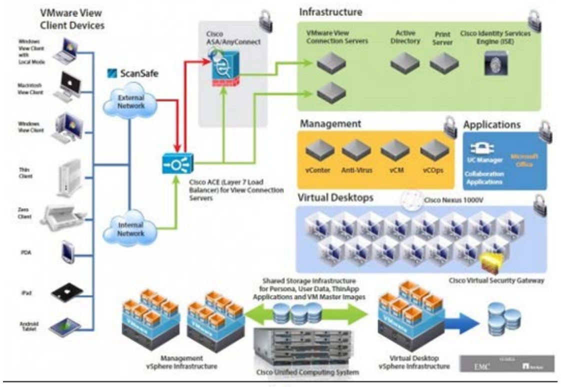
VMware View Client Devices
Windows View Client with Local Mode
Macintosh View Client
Windows View Client
Thin Client
Zero Client
PDA
iPad
Android Tablet
ScanSafe
External Network
Internal Network
Cisco ASA/AnyConnect
Cisco ACE (Layer 7 Load Balancer) for View Connection Servers
Infrastructure
VMware View Connection Servers
Active Directory
Print Server
Cisco Identity Services Engine (ISE)
Management
vCenter
Anti-Virus
vCM
vCOps
Applications
UC Manager
Microsoft Office
Collaboration Applications
Virtual Desktops
Cisco Nexus 1000V
Cisco Virtual Security Gateway
Shared Storage Infrastructure for Persona, User Data, ThinApp Applications and VM Master Images
Management vSphere Infrastructure
Cisco Unified Computing System
Virtual Desktop vSphere Infrastructure
EMC

fig. 3

Having employees access the resources of the organization by accessing a virtual desktop infrastructure built in a private cloud instance might have the opportunity to address some of the concerns. The organization can impose two or three factor authentication to login onto the VDI (virtual desktop infrastructure) environment and encryption for data in motion, in use and at rest. From that virtual desktop user can access internal resources like they were sitting to a workstation located on the premise of the organization (see above picture for the infrastructure design).

By leveraging industry leading practices, integratinga thoughtful BYOD policy and adopting strategies thatare flexible and scalable, organizations will be betterequipped to deal with incoming (sometimes unforeseen)challenges to their security infrastructure posed bythe use of employees' own devices.The introduction of appropriate procedures andregular testing will help organizations becomesmarter and make their employees more aware of thechallenges that the use of personal devices pose forthe entire enterprise.

Bibliography

[1] Jamey Heary; Aaron Woland, Cisco ISE for BYOD and Secure Unified Access, Video Enhanced Edition, Cisco Press, Jun 2013

[2] Forrester, Key strategies to capture and measure the value of consumerization of IT, July 2012

[3] www.ey.com – Bring Your Own device, Security and risk considerations for your mobile device program, Sep 2013

[4] Jessica Keyes, Bring Your Own Devices (BYOD)Survival Guide, ISBN-13: 978-1-4665-6503-6, 2013

[5] Quillen, I. (2011). Crafting your BYOT policy. Digital Directions. 23

[6] Ullman, E. (2011). BYOD and security. Technology & Learning, 31