Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 9 (2013) 43 – 53

Procedia Technology

CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies

BYOD Bring Your Own Device

Georg Disterer*, Carsten Kleiner

University of Applied Sciences and Arts, 3049 Hannover, Germany

Abstract

Using modern devices like smartphones and tablets offers a wide variety of advantages; this has made them very popular as consumer devices in private life. Using them in the workplace is also popular. However, who wants to carry around and handle two devices; one for personal use, and one for work-related tasks? That is why "dual use", using one single device for private and business applications, may represent a proper solution. The result is "Bring Your Own Device," or BYOD, which describes the circumstance in which users make their own personal devices available for company use. For companies, this brings some opportunities and risks. We describe and discuss organizational issues, technical approaches, and solutions.

Keywords: BYOD; Bring Your Own Device; Mobile; Enduser Device; Consumerization; Architecture; Mobile Device Management

1. Problem

Devices like smartphones and tablets combine several attractive features: They are easy to carry and provide access to voice and data services, thereby opening up a wide variety of potential mobile applications, "anytime and anywhere." Thus, a high level of acceptance is expected for these devices, Forrester states "…

* *E-mail address:* georg.disterer@hs-hannover.de

doi:10.1016/j.protcy.2013.12.005

mobile device adoption explodes …" [19] expecting to see 1 billion smartphone users in the year 2016, assuming that devices are used for personal use. These come along with slogans and phrases such as "… the rise of mobility and the marginalization of the PC“ and "move-and-do“ culture. For companies, Gartner recognizes a continued dramatic rise in the demand for mobile device applications until 2015, and considers the use of mobile devices in the workplace to be among the ten most important strategic trends [10].

The figures for using mobile devices for work-related tasks in 2016 are estimated at 350 million users of mobile devices, of which 200 million will be using their own personal devices for work-related tasks as well [19, 8]. This scenario is discussed under the slogan "Bring Your Own Device," BYOD, and has been drawing much attention. According to a study of McKinsey, 77% of all CIOs plan to grant employees mobile access to company data and applications [2]. This means companies are faced with the question of whether and how to manage users with own personal devices performing work-related tasks and personal devices entering the workplace in order to improve effectiveness and efficiency in data processing.

Opportunities are particularly found in the increased level of comfort, while risk is seen in technical problems, in security, and in legal questions. Striking phrases have been used in describing these risks, such as BYOD interpreted as "Bring Your Own Danger" and prophecies of "IT anarchy". Additionally, organizational rules are needed for several everyday situations.

With BYOD consumer devices enter the workplace. "Consumerization" describes the penetration of consumer market devices into business settings. This reverses the traditional manner in which innovation has spread, where new technologies are used first at companies and then users end up also employing them for private ends. Under BYOD, not technical experts at companies evaluate and select technologies for business purposes, but private users are familiar with the personal devices and their utilization in private life, and take them into work in the course of "user-driven innovation“ [12, 13]. According to a recent study by Forrester, 50% of 18- to 31-year-old and 40% of 32- to 45-year-old workers believe the technologies they use in private life is “better” than those in their professional life [11]. Thus, BYOD is showing new innovation paths for which there is a limited body of academic research.

According to research, mobile devices are already being used at around 80% of German companies for traditional telephone communication, for functions of a traditional telephone system (including short cuts, forwarding calls ...), for e-mail, and for access to centralized calendars and contact information [4]. 60% of companies in the USA and Europe have set up BYOD programs for smartphones, and 47% have done so for notebooks and tablets [9, 8]. However, these figures do not reveal the extent to which utilization goes beyond rather simple telephone communication and e-mail.

The fuzzy figures on prevalence reveal the need for differentiation. Distinctions should be made based on ownership of device and on using devices for telephone and e-mail or beyond (see Table 1). The quadrants indicate the respective degree of prevalence for German companies according to a more recent study [15].

Table 1: Using mobile devices for work-related tasks

	company-owned devices	**privately-owned devices "dual use"**
use for telephone and e-mail	… established for years e.g. Blackberry/RIM > 90% of companies in Germany	… established for years e.g. e-mail from home via Web ~ 50% of companies in Germany
use for company applications beyond telephone/e-mail	… established for years e.g. notebooks via WLAN or Web, remote access via VPN ~ 60% of companies in Germany	**BYOD** … privately-owned devices for company applications beyond telephony and e-mail ~ 33% of companies in Germany

The type of application used with mobile devices is decisive, as telephone and e-mail are run through technically mature and standardized systems for which there are known security measures. System environments must be encapsulated such that company data and applications are not exposed to risk. This makes it possible to process e-mails via a web interface without major restrictions and without company data having to be stored locally. Establishing and securing access to company data and applications beyond telephone and e-mail is generally nontrivial and expensive.

Ownership of the devices being used is decisive, as selection, installation, and maintenance fall under the company's responsibility and personal use of devices can be restricted or blocked; however, this means that users are not permitted "dual use," which implies they are expected to keep two different devices ready and to be proficient in the use of both of them. By contrast, using personal devices always permits "dual-use", as the owner of a device cannot be prohibited from using it restricted anyhow.

The table also shows that several features of BYOD are close to traditional uses of mobile devices, which means that some experiences can be used. Additionally, since years companies have external persons, like consultants and auditors, using their own devices at the company. And for quite some time, companies' executives have been granted privileged access to use their personal device in "dual-use" mode for a broad spectrum of applications.

2. Opportunities and Risks Associated with BYOD

With BYOD - using privately-owned devices for company applications beyond telephony and e-mail – some special opportunities and risks arise.

2.1. Opportunities

The most important chance of BYOD is the comfort users enjoy in using only one single device …

- "Anything": personal and business use beyond telephone and e-mail,
- "Anywhere": mobile use with a portable device connected via WLAN or Internet,
- "Anytime": use during working hours and private times.

The alternative situation is discouraging: Users switch between various mobile devices in order to execute both private and work-related tasks, or are restricted by the use of stationary devices, or carry around two (or more) mobile devices for private and business issues. Another alternative, letting employees use company-owned devices for personal use without any restrictions, bears security and compliance risks, as well as higher costs, because a larger group of employees would have to be equipped with suitable devices. Additionally, companies will hardly be able to provide a pool of equipment that can meet the high, divergent, and quickly changing demands of users experienced with consumer devices.

BYOD reacts to two momentous developments:

- The ever more diminishing boundaries between private and professional life with flexible working hours, the potential to work at home or while out and about, high demands on reachability for work outside of business hours, and higher obligations on all employees within their social network – and companies becoming increasingly considerate of these social obligations. Employees and employers are increasingly distinguishing less between personal and company time - or perhaps are more unable to distinguish between the two. These trends are supported when it becomes possible to use one single device for private and business ends alike ("dual use").
- Increasing mobile use of e-mail, Web, and applications beyond in both private and professional life: Private ownership of high quality mobile devices is growing rapidly. People use devices "anywhere" and "anytime"

for private communication to participate in social networks, or to take advantage of special offers in e-commerce. For the year 2011, approx. 20 million mobile web users have been estimated in German speaking regions [1]. Simultaneously, business use of mobile devices is growing: At around 80% of companies in Germany, mobile devices are used for traditional telephone, e-mail, and access to centralized calendars and contact information, 56% of users of corporate devices also use them for surfing on the Web [1]. A more recent study shows even more intensive use of company devices: Business applications (beyond e-mail and web) are used at 58% of companies in Germany [15].

The comfort offered by BYOD leads to a higher level of user satisfaction and productivity, which are also enforced by the following effects: Users gain a sense of autonomy from the independent procurement of devices, are more familiar with devices that they also use privately, and find consumer devices easier to use. Overall, user satisfaction and productivity is considered to be a primary advantage of BYOD [9]. Additionally, the increase in a company's attractiveness as an employer due to BYOD should be noted, which has an effect on techy young employees in particular. And BYOD facilitates the use of special personalizing functions, as devices are usually used by one single person and can therefore be customized to individual needs via stored profiles. Sensors implemented on the devices can also be used for localization.

2.2. Risks

Mobile devices currently are clear leaders in the list of the most significant security risks, as demonstrated by a study involving security experts from companies from various sectors [8]. Academic literature on BYOD concedes the most attention to security [17]. The fundamental values of confidentiality, integrity, and authenticity of company data are particularly threatened. Confidentiality is compromised when unauthorized parties obtain access to sensitive private information or confidential company information by manipulating devices or intercepting data transmissions. Manipulation performed using insufficiently secured devices threatens the integrity of company data. Authenticity is threatened when devices are used to trigger business transactions that cannot be traced clear without ambiguity.

Mobile devices that are insufficiently secured lead to unauthorized use and modification of data due to deliberate or negligent actions. When personal devices are being used, it must be assumed that the negligent or incautious behavior of users during private use will be transferred to business use. Additionally, there are legal stipulations and compliance rules on company use which must be met, such as requirements to document, archive, and back-up. Accordingly, when mobile devices are designated for BYOD access for both private and business purposes ("dual use"), the end user's private data (contacts, addresses, photos, documents) must be protected against a company's access while the company access to company data is simultaneously guaranteed. A lack of separation between private and business spheres yields significant risks for companies.

Additionally, the level of complexity of the information technology to be mastered increases when a distinction has to be made between private and business use on a large number of devices channels. This yields additional security risks, sometimes formulated to the point as "Complexity is the enemy of security" [16]. User support for BYOD may be complex and expensive due to the larger scope and increased level of complexity [7]. It can be expected that a multitude and broad spectrum of devices will have to be supported, with devices having to be exchanged more frequently than is usually the case with company devices. Users will require support in registering privately-owned devices and installing software will need help with technical frictions between personal and business use, and will expect services in case a defect occurs or the device is lost. Which procedures are planned if a device is lost (due to misplacement or theft)? How will data stored locally on the personal device be wiped-out? Will the employer provide replacement devices so that users can continue to work? May GPS be used to locate the device - even if it cannot be ruled out that a companion has taken the device accidentally?

Overall, BYOD appears to contradict some recent approaches of information management designated with terms like standardization, consolidation, and reduction of complexity. Quite the contrary: BYOD requires the management of various new and sophisticated devices with different applications.

3. Architectural Concepts and Technological Approaches

In order to facilitate the use of personal devices for business purposes, there are various architectural concepts and corresponding technological solutions available. This is particularly true for scenarios that go beyond standard applications that are already in use (see Table 1). A distinction is made based on the amount of business use intended for the personal device. In principle, these approaches are the same architectures that are used in virtualization solutions. The objective is to isolate business applications from the rest of the system. In the case of BYOD, this means isolation from other applications running on the personal device.

Figure 1 outlines the various approaches, represented as variations in the distribution of a business application between mobile devices and a company's central servers. Classic three-tier architecture is used for the principle structure of a business application, consisting of a presentation component, an application component, and a data component. For several solutions, a distinction needs to be made between the launch and execution of the application. The reasons for this will be explained in the following sections. Note that approaches marked “DL” unavoidably require local storage of business data on the device, whereas the others may do so for optimization purposes but don’t have to. Thus, the corresponding aspects of local storage could also be relevant for these approaches. The following sections describe the approaches in detail and reveal advantages and disadvantages.

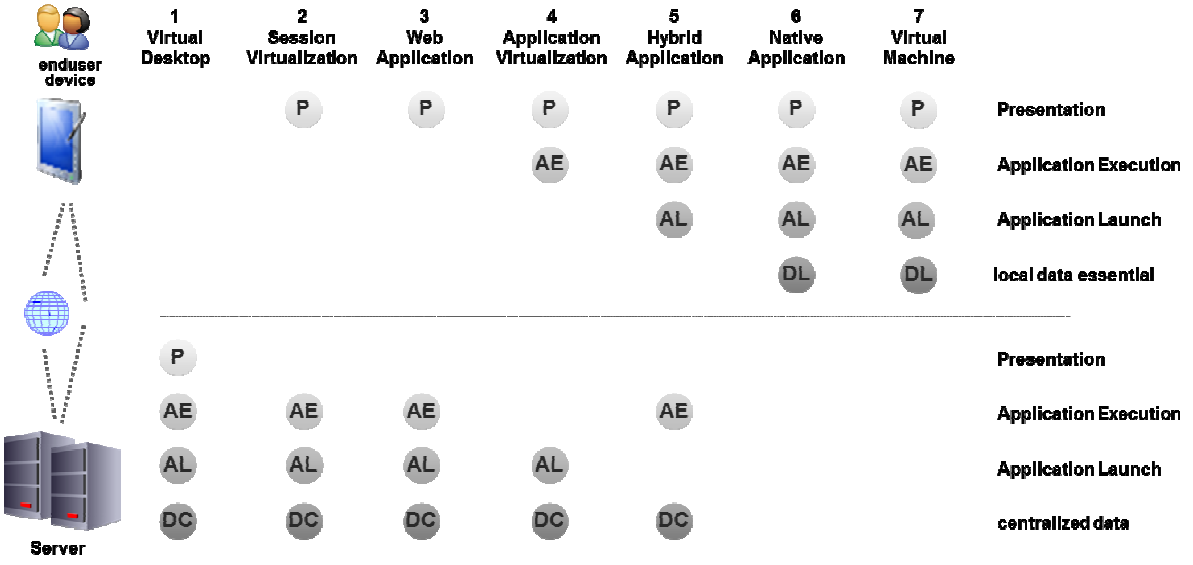

Fig. 1: Architectural Concepts and Technological Approaches

3.1. Virtual Desktop

When using a virtual desktop, the mobile device launches a virtual machine or a company application on a server in the company network. The application's user interface is generated on the server and displayed on the

device only; user interaction is also processed on the server. Thus, this approach is a mobile variation of terminal servers known from traditional desktop systems. Due to the high bandwidth and low latency required which can currently not be guaranteed in most situations we do not discuss this approach any further here. It may nevertheless become more interesting in the long term future with increased connectivity of devices.

3.2. Session Virtualization

The session virtualization approach [22] also provides the company application on a central server on the company network. A mobile device launches the application, which causes the server to generate a new dedicated session for that device and to send a generated user interface to the device. The device displays it and receives user input. The input is transmitted directly to the server, which uses it to generate and send a new user interface to the device. This kind of application provisioning is also suitable for streaming, which means it has less demand for bandwidth and, especially, latency than a virtual desktop.

One advantage is that there is no expenditure for platform-specific procurement and operation of the application; no use of platform-specific app stores, etc., is required. Since the company application is only displayed and not executed on the device, it cannot have any influence on a mobile device's system or store data locally. In the interest of securing data integrity, it should be ensured that there is a permanent, stable, and secure data connection and that the devices are not compromised. Since a dedicated session is generated on the server for each device, device-specific display of the user interface and the use of specific control elements are possible. However, this is associated with rather high implementation efforts.

The procurement and operation of an additional application provisioning infrastructure is necessary. However, this solution tends to be easier to set up than the solution with virtual desktops. It is not possible to use the application without an Internet connection. Irrespective of the technology being used in this case, the level of support found among current mobile platforms is very poor. This is especially true for the use of platform-specific interaction (such as gestures). Additionally, the use or exchange of data stored locally on the device, like contact information, is hardly possible, as it is only accessible via a local clipboard on the device.

3.3. Web Application

A web application represents a special kind of session virtualization, discussed here due to its great practical importance, especially for mobile devices [5, 3]. A web or application server is used for application provisioning. Clients use a conventional web browser that is available on all platforms. The classification shown in Fig. 1 is only valid when the web application is used for display only, e.g. with classic HTML. When using currently popular web applications featuring JavaScript or enhanced HTML5 functions, part of the application logic is executed on the device, which would be classified as a hybrid application (see Section 3.5).

The implementation of standard technologies on both the server and client inherent to web applications means that the additional effort for procurement and operation is marginal. Today, every company is running a web server anyway, and every mobile device features a web browser. Since communication is performed via https, the use of VPN can be avoided. However, note that the web application is therefore available over the public Internet. Thus, solid access protection mechanisms are necessary in order to secure data integrity. Another advantage is that the technical requirements for mobile devices are negligible and it is possible to support a large group of devices at low cost. The amount of bandwidth needed is also comparatively low, such that utilization is possible not only via WLAN, but via GSM/UMTS as well.

Compared to the solutions discussed thus far, it should be noted that many current browsers principally have the potential to access the local system. Even if one's own web application doesn't use JavaScript, the

danger associated with using these standard components is much greater than if using proprietary technology. For example, current browser data can be stored on a mobile device, thereby triggering a greater risk. Furthermore, there is more malware available based on standard technology.

Further disadvantages to web applications include the necessity of a data connection to run them, and a rather poor user experience on the device - even if that can be partially remedied with the usage of web frameworks. While there are now solutions intended to facilitate offline use of a web application, this is always associated with local storage and execution of the application on the device, such that classification as a hybrid application (Section 3.5) would be necessary. The use of specific device functions, such as sensors, is not possible with this approach. Additionally, the use or exchange of data stored locally on the device, like contact information, is hardly possible, as it would only be accessible via a local clipboard on the device.

3.4. Application Virtualization

With application virtualization [20], an executable application is provided on a server on the company network. When loading an application, the device downloads the corresponding executable file from the server and then runs it on the device - usually in an isolated area (a.k.a. sandbox or container).

The omission of standard technologies and provisioning on the company network, which is only accessible via VPN, means that unauthorized access to the application becomes much more difficult. Since each device downloads the executable file from the server, they are always working with the most recent version. This means that version management is rather easy.

The use of an isolated area on the device means that a marginal risk level can be achieved regarding other software accessing the application's data. Conversely, the company application is also largely barred from influencing the device and private data. A virtualized application can usually be implemented such that a larger bandwidth is only necessary when loading the application. Accordingly, then only a low level of bandwidth is required and subsequent offline operation is feasible.

The disadvantages of application virtualization include (as with any of the approaches) that it must be ensured that there is no malware on the device, such as key loggers or screen scrapers. Furthermore, mutual use of data, such as contacts between the device and virtualized application, can only be initiated manually by the user. Additional software is required for application provisioning.

3.5. Hybrid Application

A hybrid application [6] combines the advantages of a web application with those of a native application. Functions that can be implemented using a web application are provided by it. For functions that cannot be handled in this manner, the web application is supplemented with a component that is executed locally on the mobile device. This local component can be rendered via JavaScript or HTML functions to access the device, or via a native application component that is installed locally on the device. The former variation is usually also designated as a web application in the literature, for it is entirely provided by the web server and executed in the web browser. Within the context of BYOD and security aspects, however, this variation should be considered to be more like a native application. In contrast to a pure web application, the native component makes it possible to use device-specific functions as well. Furthermore, it is somewhat easier to realize offline operation and provide the accustomed look-and-feel on the devices.

In addition to the advantages of web and native applications, however, hybrid applications also unite their disadvantages. For example, the requirements for devices are significantly higher than with pure web applications. Furthermore, expenditure increases in order to support various platforms, even if it is simplified for JavaScript via the use of frameworks like jQuery Mobile, Titanium Mobile, or PhoneGap. There is an

additional significant effort associated with a component that cannot be implemented as a pure web application for providing the application on the distribution channel intended for the respective platform.

Executing application components on devices greatly increases threat potential, as this makes the execution of malware possible in principle. Additional security measures should therefore be planned if they aren't already being provided by the corresponding platforms.

3.6. Native Application

This solution for application provisioning [5] is currently widespread in the consumer market. An application is produced for each supporting platform in the platform's specific development environment. Applications are then provided via the corresponding distribution channel (e.g. App Store, Play Store) and audited by the distribution channel's operator, then downloaded by the user and installed locally on the device.

A significant advantage of native applications is that users receive applications with the look and feel that is typical for the platform. All specific control options can be accounted for. Additionally, utilization is possible in offline mode when all requisite data are stored locally on the device. An Internet connection is only required for installation. Even if pure offline operation is not being realized (perhaps because data would be too large or of insufficient actuality), operation is still possible with low bandwidth. Ultimately, native applications represent the only option under which company and private data can be exchanged comfortably.

However, this data exchange also leads to the greatest disadvantage of native applications. The heavy integration into the device's local system means that it is very difficult to control the separation and isolation of company and private data. On one hand most current operating systems do offer isolated execution environments for apps. On the other hand they do not prohibit, as an example, handling telephone numbers in a manner specific to the platform, such as offering the direct import of data to the local telephone book. Thus, company and private data can hardly be separated. Remote deletion of the device in the event of loss (wipe out) is only possible with a brute-force method, namely restoring the device to the original delivery state.

Another big disadvantage to native applications is that a specific application has to be implemented and provisioned for each platform. On one hand this requires extensive expertise in various different development environments and programming languages. On the other hand the complicated conditions and provisioning processes stipulated by the operators of platform-specific distribution channels have to be well known. Overall, this dependency on the operators of platforms and distribution channels represents a large investment risk. It is partially reduced with the provisioning of special, so-called company stores. However, operators also often impose specific conditions and restrictions to their benefit in these company stores as well. Ultimately, there is a high effort associated with maintaining and managing application versions and with the procurement and provisioning of versions of the platform. Additionally, there is the risk that a platform will soon no longer be widely demanded, or that manufacturers move development into incompatible directions.

3.7. Virtual Machine

The concept of a virtual machine [21] expands the idea of application virtualization to platform virtualization. An entire system is stored in one or multiple files on the device as a virtual machine, including application logic. This generally does not occur at the time the system is loaded, rather during a prior dedicated installation process. Execution of the virtual machine occurs in an area (sandbox or secure container) that is isolated and secured by the device. This procedure is a well-recognized and established process for desktop systems to secure the execution of third-party applications. Similar concepts are used by recent mobile device platforms such as Blackberry 10 specifically designed for enterprise use.

The most important advantage of a virtual machine is that the application can be run offline following prior installation of a virtual machine and player software. In contrast to application virtualization, which provides only one application, it is now possible to provide various applications simultaneously. Furthermore, the same virtual machine can be used for all platforms, guaranteeing a broad spectrum of potential utilization. Execution in an isolated area on the device means integrity is secured for both company and private data, for there is no interaction between the virtual machine and the physical device. A complete deletion of company applications and data in the event of device loss (so-called wipe out) will be easy to perform by erasing the virtual machine file, which may also be possible via remote access. In principle, it's possible to have a look-and-feel native to the device, for a complete user interface is being provided. However, this yields additional expenditure in procurement and provisioning.

The largest disadvantage to virtual machines is that the capacity for broad utilization is only established if the runtime environment for the guest system is available on the various devices. At current, there is no universal runtime environment available for mobile platforms. In light of the tremendous success of virtual machines on desktops, one can count on seeing swift development here in the years to come. Furthermore, there is a certain level of effort associated with keeping applications on the device up-to-date (as well as with maintenance and service), for example with device management software (mobile device management, MDM). For virtual machines – as for all approaches -, it is urgently recommended to secure the integrity of the native operating system on the device anyway.

3.8. Comparison of Approaches

Some conclusions can be drawn comparing the approaches described so far. The greater the share of the application executed on the mobile device (in Figure 1 from left to right) increasing benefits exist because …

- the better the application can be tailored to the platform's specific user interface model. One significant advantage of using personal devices is that users can use the devices they know from private use with device-specific control options (e.g. gestures) in the accustomed look.
- the easier implementation is on server side, because less application logic has to be implemented there.
- the easier application installation and maintenance becomes on the device, because the platforms' existing distribution channels can be used. This also true for delivering updates.
- the easier an implementation of offline-capable applications becomes possible. The larger the share of the application on the mobile device is, the more functionality can be provided in offline mode.

On the other hand: The greater the share of the application executed on the mobile device (in Figure 1 from left to right) increasing drawbacks exist because …

- the more complex it becomes for the company to implement, install and maintain the application, as several platforms have to be accounted for. For each of those platforms, special development expertise is required, and specific applications and/or application components have to be implemented. Different distribution channels have to be accounted for and server-side software must be capable of handling different clients working with different application versions.
- the more important it becomes to ensure data security on the device, as there is high threat potential. Firstly important company data is stored locally on the mobile device. Secondly threat grows with the number of platforms being used, as all of them are exposed to specific malware programs.
- the greater the effort becomes for ensuring data security on the device. Due to the increased complexity there are specific security features necessary for each platform. Furthermore, locally executable applications or application components have to be secured themselves; this task is in part facilitated by employing corresponding commercial frameworks.

The pros and cons of the approaches counterbalance each other and should be measured carefully when making a decision. Lower development effort associated with the solutions Virtual Desktop, Session Virtualization and Web Application (no. 1 through 3 in Figure 1) is significant, as a single implementation can be used for multiple platforms. Conversely, the necessities of a stable and permanent Internet connection and the restricted options for tailoring to platform-specific user interfaces represent significant disadvantages.

For all approaches, it is necessary to encrypt all communication between server and device as well as all data stored locally on the device in the interest of protecting integrity of company data. However, even this cannot fully prevent data leakage, because users can still copy data to a clipboard and further on from there, be it intentionally or mistakenly. Additionally, it will be very difficult to ensure protection of the user's private data on the device against company access.

4. Mobile Device Management

For all approaches, it must be ensured that the operating system on the devices being used is not compromised by malware. When using personal devices, this cannot be taken for granted. Rather, targeted monitoring is required for this issue. Additionally, it is recommended to implement VPN or another type of encrypted communication with restricted access to the company network for the communication between devices and servers. All the devices with access to company networks and applications should be registered and administered centrally by the company. Companies should have the ability, especially when data is stored locally, to erase all company data from a device (remote wipe out) when access to data should no longer be granted (e.g. loss or theft of device, end of employment).

All this together shows why in all approaches companies should be using software for managing the devices, known as mobile device management, or MDM. Mobile Device Management represents a central point of administration of all mobile devices (including personal devices) being used at a company with regard to company issues. There are already numerous products available on the market for this matter, offering functions such as central device management, logging, monitoring, and reporting, simple installation of applications on devices, checking devices for integrity, protecting devices from malware, central control of device settings, role-based authorization system for access control [16, 14].

Selecting an MDM product requires careful consideration of a company's specific requirements. This should include an audit of the impact the chosen product will have on the rest of the IT infrastructure. A recent study by Gartner [18], for instance, considers the following products to be highly developed and promising: MobileIron, Airwatch, Fiberlink, Zenprise, Good Technology.

Despite all of the technical measures undertaken, users will always represent a significant weakness to any security concept. That is why thorough training of future users is important when implementing BYOD [16]. This also includes compulsory definition of and compliance with company-specific guidelines.

References

[1] Accenture (Edt.), 2011. Mobile Web Watch 2011 - Die Chancen der mobilen Evolution.
[2] Akella, J., Brown, B., Gilbert, G., Wong, L., 2012. Mobility Disruption: A CIO Perspective, in: McKinsey Quarterly, Sept., pp. 1-4.
[3] Anthes, G., 2012. HTML5 leads a web revolution, Communications of the ACM, 55, pp. 16-17.
[4] Berlecon (Edt.), 2011. Enterprise mobility 2011 - Bestandsaufnahme und Investitionspläne in deutschen Unternehmen.
[5] Charland, A., Leroux, B., 2011. Mobile application development: web vs. native, Communications of the ACM, 54, pp. 49-53.
[6] Christ, A.M., 2011. Bridging the Mobile App Gap, Sigma Journal - Inside the Digital Ecosystem, Oct., pp. 27-32.
[7] D'Arcy, P., 2011. CIO Strategies for Consumerization: The Future of Enterprise Mobile Computing. Dell CIO Insight Series.
[8] Deloitte (Edt.), 2011. Raising the Bar - TMT Global Security Study.

[9] Forrester (Edt.), 2012. Key Strategies to Capture and Measure the Value of Consumerization of IT - Enterprises Achive a Wide Range of Benefits by Deploying Bring Your Own Device Programs.
[10] Gartner (Edt.), 2012. Hot Research Circle: Hot Topic Survey Results.
[11] Gray, B., 2012. Building A Bring-Your-Own-Device (BYOD) Program, Forrester Research (Hrsg.).
[12] György, A., Cleven, A., Uebernickel, F., Brenner, W., 2012. Exploring the Shadows: IT Governance Approaches to User-Driven Innovation, Proc. of the 20th European Conference on Information Systems ECIS. pp. 1-12.
[13] Harris, M., Patten, K., Regan, E., Fjermesat, J., 2012. Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?, Proc. of the 18th Americas Conference on Information Systems (AMCIS), pp. 1-7.
[14] Hemker, T., 2012. Ich brauche das! – Mobile Geräte im Unternehmenseinsatz, Datenschutz und Datensicherheit, 3, pp. 165-168.
[15] IDC (Edt.), 2012. Managing Mobile Enterprises.
[16] Johnson, K., 2012. Mobility/BYOD Security Survey. SANS Institute (Edt.).
[17] Niehaves, B., Köffer, S., Ortbach, K., Katschewitz, S., 2012. Towards an IT Consumerization Theory - A Theory and Practice Review. ERCIS Münster (Edt.).
[18] Redman, P., Girard, J., Basso, M., 2012. Magic Quadrant for Mobile Device Management Software, www.gartner.com/id=2019515. 2012-11-19.
[19] Schadler, T., McCarthy, J. C., 2012. Mobile Is The New Face Of Engagement - CIOs Must Plan Now For New Systems Of Engagement. Forrester (Edt.).
[20] Subar, S., 2010. Mobile virtualization – coming to a smartphone near you. www.visionmobile.com/blog/2010/06/mobile-virtualization-coming-to-a-smartphone-near-you. 2012-11-19.
[21] Texiwell, N., 2011. Get Your OS from VMware: Mobile Virtualization Platform. www.virtualizationpractice.com/get-your-os-from-vmware-mobile-virtualization-platform-11080. 2012-11-19.
[22] Tulloch, M., 2011. VDI vs. Session Virtualization. www.biztechmagazine.com/article/2011/04/vdi-vs-session-virtualization. 2012-11-19.