HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

THE NEED FOR BYOD SECURITY STRATEGY

A BYOD ESZKÖZÖK BIZTONSÁGI STRATÉGIÁJÁNAK IGÉNYE

KADËNA, Esmeralda; KOVÁCS Tibor

(ORCID: 0000-0002-3808-6909); (ORCID: 0000-0001-7609-9287)

kadenaesmeralda@gmail.com; kovacs.tibor@bgk.uni-obuda.hu

Abstract

With the recent advancements in technology and the rapid adoption of smartphones, tablets and laptops, it has become increasingly common for employees to use their own personal devices to perform work-related tasks. This is known as Bring-Your-Own-Device (BYOD). Permitting employees to utilize their own preferred device in the work-place also brings some risk of data loss for the enterprises, whether by employees losing devices or compromising cybersecurity.
This work is based on literature reviewing and two research questions are held: "What are the security risks associated with implementing BYOD in the workplace?" and "What are best practices to create a BYOD strategy in workplace?". Formulating a BYOD strategy is only one side of the equation, the other is the employee education.

Keywords: *BYOD, security risks, strategy.*

Absztrakt

A technika újkeletű fejlődésével, az okostelefonok, tabletek és laptopok gyors átvételével egyre elterjedtebb lett a munkavállalók körében, hogy saját személyes eszközeikkel hajtsanak végre munkához kapcsolódó feladatokat. Ezt a jelenséget BYOD-ként ismerjük (Bring Your Own Device: hozd a saját eszközödet). Az alkalmazottak számára annak engedélyezése, hogy saját, előnyben részesített eszközeiket hasznosítsák az munkahelyen, a vállalati adatvesztés kockázatát is magában hordozza, akár az eszköz elveszítésével, akár a biztonság veszélyeztetése által. Jelen munka a vonatkozó irodalmi áttekintésen alapul, miután két kérdést vet fel: Melyek azok a biztonsági kockázatok, amelyek a BYOD munkahelyi bevezetésével együtt járnak? Valamint: Melyek azok a legjobb gyakorlatok, amelyek a BYOD stratégia munkahelyi megteremtésére irányulnak? A BYOD stratégia megteremtése a kérdés csupán egyik oldala, a másik a munkavállalók oktatása.

Kulcsszavak: *BYOD, biztonsági kockázat, stratégia*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.12.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.22.

INTRODUCTION

Nowadays the use of the Internet has assumed omnipresence, affecting the way we live and work. New concepts and concerns come with it and here I will concentrate on the emerging concept of Bring-Your-Own-Device (BYOD). According to the defining of Ghosh et al., BYOD is a new development in the workplace through which the employees are encouraged to access organization resources like corporate e-mails, calendars and scheduling, documents, applications, etc., with their personal devices, either for work or for personal use [1].

The relative low cost of the smartphone and also its ease of use at the workplace for voice and data services, contribute also to the adoption of BYOD concept. The characteristics of smartphone have to do with its contemporary advanced features and the numerous applications (apps). From the point of view of computer architecture, basically it is an embedded portable computer, equipped with interactive, mostly Java-based Apps, running on flexible operating systems (OSs) such as Android, iOS, Windows Mobile, etc. The paradigm of running these smartphones on mostly free-and open-source software (FOSS), have made its adoption and use very reliable and universal [2].

According to this, different organizations are coming to terms with the need for a BYOD strategy to authenticate and authorize employees to use BYOD on enterprise networks, which would inure to the benefits of the organization. On the other hand, BYOD presents network externalities which could impact on the corporate security framework of re-defining the uncertainties of network perimeter and to safeguard the information assets to ensure confidentiality, integrity and availability (CIA) [3], [4].

A key concern with BYOD is the case where management of the organization may not be aware of personally-owned devices accessing corporate resources. Furthermore might happen that the needed technical support may not also provided. According to past related- studies, it is shown that there is an increased cyber-risk posed to the sensitive corporate information assets of any business when "foreign" and/or unauthorized devices access the corporate network [5].

The research of Onwubiko and Owens shows that employees compliance with security policies and guidelines is taken for granted in many companies. Instead they prefer a formalistic approach of the security [6]. Actually these provides some directives on where to extra resources should be used to improve the employees (regarding security awareness) as one of the most important lines of the defense. A compromised mobile device with access to the enterprise network could serves as vulnerable entry points for nefarious activities within the network and possibly with access to sensitive information. Therefore is very important for any organization while adopting BYOD, to put in place the appropriate security measures in order to mitigate against the disadvantages of this phenomenon.

It was reported that in a study from Alcatel-Lucent's Motive Security Labs, 16 million mobile devices worldwide have been infected by malware and mobile infections are said to be growing at a disturbing rate, with an increase of 25% in 2014 comparing with 20% in 2013 [7]. CEBR reported that mobile-related cyber-attacks cost UK businesses about £18 billion in lost revenue and £16 billion in increased IT expenditure per year resulting from breaches [8]. As we can see, the report indicates that the mobile devices compromises are a widespreas risk, where 81% of UK businesses recording a breach in 2014 [8].

Actually experts believe that if nothing is done about the cyber-risk threats, the organizations in all parts of the world are faced with cybersecurity breaches and will continuously remain faced with these concern. These breaches resulting mostly in breach cost such as incident response forences, clean up, legal; reputation and brand damage as a consequence; and lost on their revenue due to downtime and so on [3]. To aggravate the already unsafe situation, the major part of SMEs in developing economies consider

themselves as not having any data attractive to threat agents, and they have not face any attack. Actually the contrary is true, it can be imagined/believed, big companies usually have data on employees, clients, suppliers, partners, etc., and it is with much more interest for attackers to have that large information on their hands [3]. Although this, there are no limits for attackers, the potential risks and countermeasures to stay on the safe side should be taken not only in consider but also to implement them in the appropriate way.

BYOD CHALLENGES AND SECURITY RISKS

The BYOD concept implemented in different kind of organizations can bring about many advantages such as increased efficiency and convenience. But what might be convenient for us (users) can be also convenient for attackers. Thus this phenomenon as it was mentioned above led to/bring a number of security risks for IT infrastructure and data of the enterprises and users also.

Actually there are certain factors that increase the occurrence of BYOD risks. To start, when the enterprise and personal data are allowed to coexist on the same device, then it becomes very problematic and challenging to find a balance between security control of enterprise and privacy of personal data, especially when the device is not a corporate asset. Furthermore, it is not easy for IT departments to support different phone/OS version/carrier combinations [9], which are also constantly changing with technical advancement and get outdated very quickly [10], [1], [11]. We should also keep in mind that because of the increased processing power and memory of smartphones and tablet computers, increased data transmission capabilities of the mobile phone networks, and open and third-party extensible operating systems for mobile devices, they become an interesting target for attackers [12].
Below are listed and more explained some associated risks related with BYOD in enterprises.

Data leakage

Data Leakage can result from different causes. Considering a lost/stolen device case. Data leakage can happen when an attacker access data on a lost or stolen device with unprotected memory. If data on the BYOD memory or its removable media is not adequately secured by encryption it is possible that an attacker can easily gain access to information [13]. Another case is when enterprise information is sent to personal contacts by mistake [11]. Usually and very often BYODs contain also important and valuable information such as credit card data, bank account numbers, passwords/PINs and so on. Because of their portable nature, they are the main store for the user's personal information and also corporate sensitive data. Moreover there are chances that some disgruntled employees may also share confidential business data on personal devices with competitors, leading to a competitive disadvantage for the organization [1].

Another case has to be with improper decommissioning. It means the transfer of a mobile device to another user without removing sensitive data may result in an attacker gaining access to the data on it [5]. Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives prior to decommissioning. Unfortunately, the same is not yet happening with mobile devices used in the workplace with sensitive corporate data.

Reminding that personal devices are not part of the business's IT infrastructure, and due to that, these devices are not protected by company firewalls and systems (unless the company takes countermeasures against this). So it is clear that data leakage can led to not only problems for users but through BYOD they can be transmitted also to company causing company's system vulnerable to data breaches.

Data Disclosure by accident

It is possible that data can be disclosed unintentionally by the user of a mobile device. Data is transmitted or received and many users are either unaware, tend to forget that or ignore the privacy settings. Even though they may have given a clear approval, their naivety about functionality of device applications led to problems with their awareness on the fact that an application collects and publishes personal data [3], [14].

Phishing and SMishing

Phishing or SMiShing can result from an attacker using phony applications, SMS, or email that appear unpretentious to collect user credentials like password, PINs, or credit card information [15]. Phishing attacks are well-known threats for users of traditional computers and are increasingly becoming a concern for mobile devices and platforms alike for several reasons. What is more, the reduced screens sizes of these devices, makes it convenient for attackers to camouflage useful hints like whether the website uses SSL, that users rely on to decide whether or not to submit credentials. Also, application stores provide a new way of phishing by giving attackers the chance to place counterfeit apps in the app-store, looking like authentic apps, as well as these devices provide additional channels that can be used for phishing, using SMS in the case of SMiShing. Users may be less cautious about SMS phishing messages, and finally even though users may be aware of the risk of phishing in traditional computers, most are unaware of the same type of risk in mobile devices.

Hackers can infiltrate system

It can result from network resource overload due to many mobile devices connecting to the corporate network and exhausting resources and making them unavailable to legitimate users. Thus, the availability security dimension is said to have been compromised of breached. The uptake of smartphones usage and mobile Internet, have increased the risk of network congestion through either signaling overload or data capacity overload [16].

Network congestion

Vulnerabilities

Several kinds of vulnerabilities still remain a crucial concern for BYOD. It was reported from Enterprise Apps Tech News, that CyrusOne outlines malware, device theft and phishing as among the key risks for organizations [17].

Malware: There are many types of malicious software (malware) and are referred to by different names depending on the function. It tends to disturb users by entering at private specific information, they may cause breakdown of the device and lead to stolen or to become unusable the information/documents of the users [18]. Common malwares include Spyware, Virus, Financial Malware, Surveillance Malware, Trojan horse, etc. They are a big problem when implementing BYOD strategies into a business. While using personal devices, employees can access whatever sites or download any mobile applications that normally business would restrict to protect its system.

"Jailbreaking" or "rooting" a device also puts company's systems at risk because it removes limitations imposed by the manufacturer to keep the mobile software updated and protected against external threats. It's best to understand that as employees have the freedom to choose whatever device they want to work with, the process of keeping track of vulnerabilities and updates is considerably harder. Through this method hackers are allowed to have access to the OS of the mobile and as a result creates a vulnerability. Furthermore

these devices do not receive the necessary security updates and become vulnerable to threats [19].

POSSIBLE SOLUTIONS AND STRATEGY

Taking in consider that BYOD is applied in many companies and the risks and challenges that this phenomenon brings, it is very important for organizations, especially for IT departments to have a strategy to create a balance between a great user experience and effective information security.

To avoid risk one option might be the strategy of "Here is your own device (HYOD)". Here the devices are provided by the organization where the enterprise has total control on the device. It can happen that employees are resistant against this approach and they may use workarounds as using a company-owned device may be considered inconvenient for them [20]. Furthermore Earley et al., note "the trick is to use transparent approaches and a light touch, rather than intrusive approaches that will only encourage workarounds" [21].

An acceptable use policy may be used alone or in conjunction with installed software for managing the device [22]. In case that a software option is chosen, then a mobile device management (MDM) application can enforce the policies required by the organization prior to providing the employee's device with access to the company network [20]. It was noted from Chang et al., that the "BYOD policies include identifying which devices can be used in the company network, listing both allowed and banned apps, and describing classes of data that shouldn't be stored locally after being used by a mobile application" [20, p. 2]. A whitelist and blacklist of applications should be maintained with an understanding that the blacklisted applications will never be installed on a managed device [1].

In case the device is lost or stolen the user need to back up his/her personal information before and during enrollment in the MDM [23]. The MDM should adhere to the company security policy to enforce passwords and screen lock capabilities also.

The U.S. White House suggests three virtualization methods:

- Remotely access the computing resources so the data is not stored on the personal devices;
- Implement a walled garden that separates the personal and corporate apps processes;
- Apply limited separation of the employee personal and corporate data with a requirement of security controls [20].

It was suggested by Ackerman [22], that: "keeping corporate data on the device in a separate software container (which allows the user's and the business's programs to run simultaneously without accessing each other's data)". Can be taken in consider also mandatory installation of security software, configuration of auto-update for software updates and security patches, the creation of security codes, the use of VPN protocols when using public Wi-Fi connections, the encryption of all company data, and the enabling of remote deletion capabilities.

Another important issue is related with employees and their responsibilities regarding securing policies. Their security awareness should be taken in consider in every enterprise. Organizations and especially IT departments need to create material to train their employees on different practices such as:

- What devices will be supported?
- What mobile operating systems (Android or iOS) will be supported?
- What apps, if any, will be supported?
- Address security issues with BYOD policy, including:

- Password policies;
- Public Wi-Fi security and awareness;
- Loss and/or phone theft policies.

Employees need to understand how security threats affect them personally in order to have successful operations. Why not considering the possibility that employees can should also sign an agreement after completing BYOD training to eliminate any future questions about ownership, loss, or confidentiality breaches.

Despite the effort governance, compliance and security functions put into managing information security, employees often remain the weakest link in an organization's defense. But even a basic level of risk understanding and awareness can prevent simple failures in control that are often the root cause of security breaches. This doesn't mean to force them to read and agree the policies. It is about connecting different integral parts within organization and explaining why is really important to stay in the safe side.

After a two-year transition, from May 2018, General Data Protection Regulation (GDPR) will come into effect [24]. It aims law updating to better address challenges of privacy for a better security protection for individuals and companies. And BYOD will meet it as well. Companies with inappropriate BYOD policies may run the risk of non-compliance with GDPR and paying up to 4% of global turnover, as well as the risk of insider threat and data breaches [25]. So the need to strengthen BYOD policies must be to the top of priority list and it is needed that these policies must be conform to industry regulations and correctly implemented, especially into employee training.

CONCLUSIONS

This work was developed with focus on BYOD concept. Constantly organizations attempt to improve their strategies for better management and higher returns. But one of the major challenges they must take not only in consider but also to prevent is bring your own device (BYOD) risk. It was presented that this phenomenon brings a number of security risks for IT infrastructure, data of the enterprises and users also.

The occurrence of BYOD risks are increasing and there are certain factors. Starting from the fact that the enterprise and personal data are allowed to coexist on the same device, then it becomes very problematic and challenging to find a balance between security control of enterprise and privacy of personal data, especially when the device is not a corporate asset. Maybe the balance will never be created as the technology is becoming more and more convenient and in the same time risky. But always should be taken countermeasures. Organizations and especially IT departments should have a strategy to create a balance between a great user experience and effective information security. HYOD might be a solution but it is shown that is same cases employees are resistant against this approach.

In the case of BYOD a MDM application can enforce the policies required by the organization prior to providing the employee's device with access to the company network. Also the employee's awareness is a big problem. The really intention is not to enforce but to put them and companies in the safe side. Their collaboration is needed and the companies should put more emphasize on the security training.

These policies are mentioned as solutions on in this work but normally they might have some limitations. So the future work might be providing a best view of security risks of BYOD and to see how the BYOD policies are changing and how will they change, when GDPR will come into effect.

BIBLIOGRAPHY

[1] P. K. GAJAR, A. GHOSH AND S. RAI, "Bring Your Own Device (BYOD): Security risks and mitigating," *Journal of Global Research in Computer Science*, vol. 4, no. 4, April 2013.

[2] G. HOGBEN AND M. DEKKER, "Smartphone Security: Information Security Risks, Opportunities and Recommendations for Users," ENISA, London, 2010.

[3] E. O. YEBOAH-BOATENG, "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)," Institut for Elektroniske Systemer, Aalborg Universitet, Aalborg, 2013.

[4] ERNST & YOUNG, "Security & Risk Considerations for your Mobile Device Program," EY, 2013.

[5] E. O. YEBOAH-BOATENG, "Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies," *International Journal of Electrical & Computer Sciences,* vol. 12, no. 5, pp. 20-31, 2012.

[6] C. ONWUBIKO, T. J. OWENS, "Situational Awareness in Computer Network Defence: Principles, Methods and Applications," IGI Global, 2012.

[7] P. PAGANINI, "More than 16 million mobile devices are infected worldwide," Security Affairs, 2015.

[8] CEBR, "The business and economic consequences of inadequate cybersecurity," Centre for Economics and Business Research Ltd, 2015.

[9] C. ROSE, "BYOD: An Examination of Bring Your Own Device in Business," *Review of Business Information Systems – Second Quarter 2013,* vol. 17, no. 2, pp. 65-70, 2013.

[10] E. B. KOH, J. OH AND C. IM , "A study on security threats and dynamic access control technology for BYOD, Smart-work Environment," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong, 2014.

[11] C.-C. CHANG, W. CHENG-CHIEH AND S.-C. CHEN, "The Influence of Bring Your Own Device on the Psychological Climate at Workplace," in *ICEC '14 Proceedings of the Sixteenth International Conference on Electronic Commerce*, Philadelphia, PA, 2014.

[12] G. COSTANTINO, F. MARTINELLI, A. SARACINO AND D. SGANDURRA, "Towards enforcing on-the-fly policies in BYOD environments," in *9th International Conference on Information Assurance and Security (IAS)*, Gammarth, 2013.

[13] B. CAUSEY, "Strategy: How to Conduct an Effective IT Security Risk Assessment," InformationWeek Reports, 2013.

[14] M. E. WHITMAN AND H. J. MATTORD, Principles of Information Security, 4th ed., Boston, MA: Cengage Learning, 2011.

[15] E. O. YEBOAH-BOATENG AND P. M. AMANOR, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 5, no. 4, pp. 297-307, April 2014.

[16] A. T. KARYGIANNIS AND L. OWENS, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," National Institute of Standards and Technology (NIST), 2002.

[17] J. BOURNE, "Malware and 'connection hijacking' remain biggest BYOD risks, report warns," Enterprise Apps Tech News, 2016.

[18] A. FELT, M. FINIFTER, E. CHIN, S. HANNA AND D. WAGNER, "A survey of mobile malware in the wild," in *Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2011.

[19] P. RUGGIERO AND J. FOOTE, "Cyber Threats to Mobile Phones," United States Computer Emergency Readiness Team (US-CERT), 2011.

[20] M. J. CHANG, P.-C. HO AND T.-C. CHAN, "Securing BYOD," *IT Professional,* vol. 16, no. 5, pp. 9-11, 24 September 2014.

[21] S. EARLEY, R. HARMON, M. R. LEE AND S. MITHAS, "From BYOD to BYOA, Phishing, and Botnets," *IT Professional,* vol. 16, no. 5, pp. 16-18, 2014.

[22] E. ACKERMAN, "The bring-your-own-device dilemma: Employees and businesses seek to balance privacy and security," *IEEE Spectrum,* vol. 50, no. 8, pp. 22-22, August 2013.

[23] P. FIORENZA, "Mobile Technology Forces Exploration of Bring Your Own Device," *Public Manager,* vol. 42, no. 1, p. 12, 2013.

[24] Council of the EU, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Council of the European Union, Brussels, 2015.

[25] S. BLACKMER, "GDPR: Getting Ready for the New EU General Data Protection Regulation," InfoLawGroup LLP, 5 May 2016. [Online]. Available: https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/.