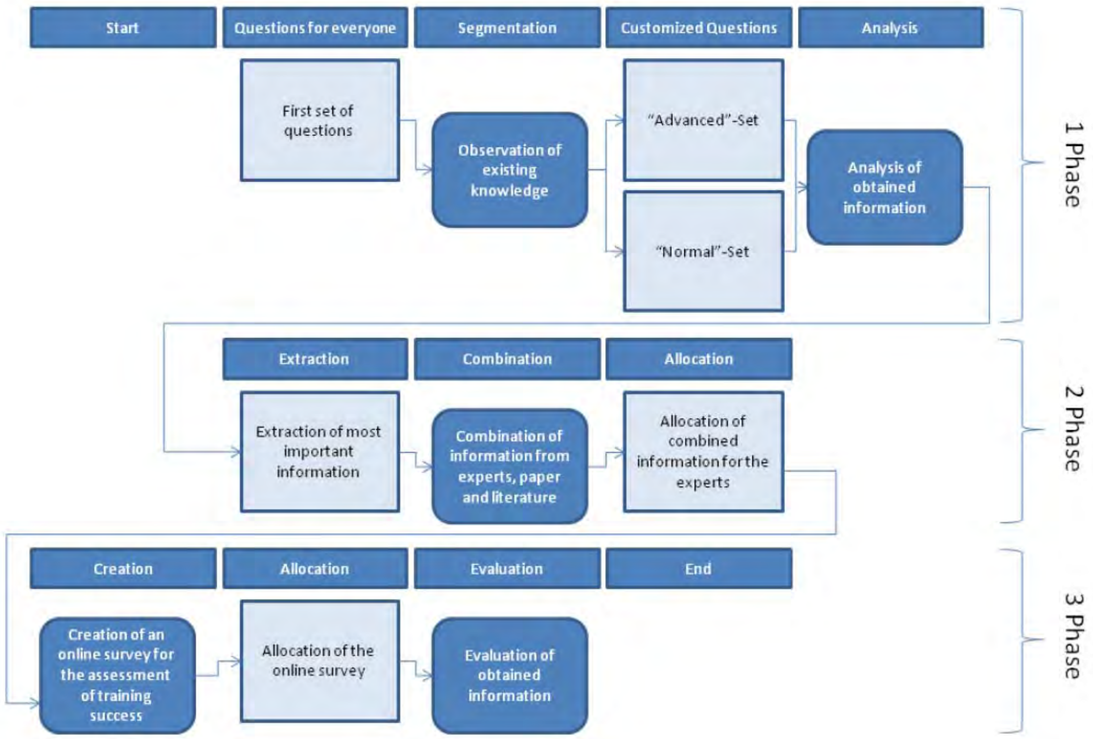
IWI Diskussionsbeiträge
# 67 (15. Juni 2015)[1]
ISSN 1612-3646

Design and Evaluation of a Mobile Security Awareness Campaign – A Perspective of Information Security Executives

Mathias Ammann[2], **Nadine Guhr**[3],
und **Michael H. Breitner** [4]


Start
Questions for everyone
Segmentation
Customized Questions
Analysis
First set of questions
Observation of existing knowledge
"Advanced"-Set
"Normal"-Set
Analysis of obtained information
1 Phase
Extraction
Combination
Allocation
Extraction of most important information
Combination of information from experts, paper and literature
Allocation of combined information for the experts
2 Phase
Creation
Allocation
Evaluation
End
Creation of an online survey for the assessment of training success
Allocation of the online survey
Evaluation of obtained information
3 Phase

[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).
[2] Student der Wirtschaftswissenschaften an der Leibniz Universität Hannover (mathias.ammann@gmx.de)
[3] Akademische Rätin, Institut für Wirtschaftsinformatik (guhr@iwi.uni-hannover.de)
[4]Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik (breitner@iwi.uni-hannover.de)

Abstract

Information security is one of the top issues for researchers and practionioners wherein the mobile security so far received less attention. In recent years, the availability of mobile and ubiquitous services has significantly increased due to the different forms of connectivity provided by mobile devices, so companies and security executives have to deal with this important issue. Many organizations and companies already implement security awareness campaigns to provide their employees awareness of these risks and to make them aware of it. But, in this paper, we focus on the perspective of information security executives. A three stage research process was carried out, which included expert interviews, an awareness workshop, and a final online survey. The results suggest that, all participated security executives gained their personal level of awareness. While before nearly all experts were not aware of sharing knowledge and the importance of being a role model, they do share their knowledge now with other employees and do accept the concept of mutual motivation.

Keywords: Mobile Security, Awareness Campaign, Information Security Executives

1 Introduction

In the early 1990s Mark D. Weiser gave the world a prediction about ubiquitous computing and how this concept would be part of everyday life in future. He mentioned the term ubiquitous computing first in his paper, "The Computer for the 21st Century" from 1991 and it means nothing less, than the omnipresent of information. Back at this time just less people were thinking about the issue of mobile security (Weiser, 1991). But in recent years, the availability of these mobile and ubiquitous services has significantly increased due to the different forms of connectivity provided by mobile devices (La Polla et al. 2013). The amount of mobile devices increases rapidly and so enterprises and security executives have to deal with this important issue. This pertinence is also caused by the fact, that today nearly everyone uses a smartphone or tablet PC for business or private activities as well. The number of sold mobile devices is still growing. While in 2012, just 725.8 million smartphones and 144.2 million tablet PCs were sold worldwide, the number of sold mobile devices gained in 2013 even more rapidly. In just one year, the number of sold smartphones gained to 1010.1 million and of tablet PC to 221.3 million devices. A prediction from 2013 says that just four years later, 1685.8 million smartphones and 386.3 million tablet PCs could be sold (Statista, 2014). This enormous number of devices underlines the increasing importance of a safe handling of mobile devices, improvement of leadership style and the necessity of precautions. The increasing number, quality and complexity of malware provide a huge challenge for enterprises (La Polla et al., 2013). This is also true for mobile devices. Enterprises are exposed to high risks like malware, which increase rapidly (Sabeeh et al., 2011). This is the reason why enterprises try to protect their information systems by several security measures; but they also have to make sure, that all employees act safely (Dagon et al., 2004) because the human factor is often even more essential. Different studies are concentrating their attention on the human factor (Fox, 2003). Those studies are showing that not just criminal energy causes damage to enterprises, but also a lack of knowledge in regard to sensitive data (of employees) and the incorrect handling of a mobile device. They are elucidating the importance of an interaction between technology and human behavior. This is the reason why a loss of a device is also a huge risk, enterprises have to deal with (Singh, 2012). Because of a rapidly increasing currentness and the fact that today nearly everyone is related to this topic, makes awareness for a safe handling of mobile devices, such an important issue. This raises several questions about the capabilities of an awareness campaign, to train employees, to act more safely, while dealing with sensitive data. This study investigates the following research questions:

R_1: Are information security executives already well trained in terms of security problems of mobile devices, or has an awareness campaign some effects on their performance?
R_2: Is an awareness campaign able to affect the safety behavior of information security executives, or are other target groups more relevant for such a campaign?
R_3: Are information security executives trained and educated by an awareness campaign, able to relay their skills and knowledge of information security behavior to other employees for a better understanding of data integrity and a safer handling of mobile devices?

The paper is organized as follows. Section 2 introduces some background notion on the importance of awareness in the context of mobile security. Subsequently, the research design is described. After presenting the analyzing methods for the literature review and the interviews, we report the results. Following the discussion and implications for research and practice, we conclude by pointing out limitations and giving an outlook for further research.

2 Theoretical Background

2.1 Mobile Device

Because of the reason, that there is no global and consistent definition of the term "mobile device" it is necessary to take a closer look by identifying an example. According to dictionary.com, a mobile device is "A portable, wireless computing device that is small enough to be used while held in the hand; a hand-held: a large selection of smart phones, PDAs, and other mobile devices" (Dictionary.com, 2014). A second definition comes from the "Mobile Commerce Report" of Durlacher Research Ltd. combined with the research of Markus Tschersich and describes three out of seven attributes of mobile communication: ubiquity, reachability, security, convenience, localization, instant connectivity and personalization (Durlacher, 1999). Out of these seven, three attributes (localization, reachability and ubiquity), are considered as the main three (Tschersich, 2012). With the help of these three attributes it is possible to create a matrix, where several devices can be classified. Only devices with a high rating in localization, reachability, and ubiquity are defined as "mobile device" (Tschersich, 2012). This technique is very helpful, because even a new kind of device (not released yet), can be classified with the support of this matrix without any effort. According to Tschersich, only devices which have high ratings in all three categories can be defined as a mobile device (Tschersich, 2012).

personal straights and their weaknesses in regard to mobile devices. Then the weak points were filtered out and a solution was considered, how their knowledge and behavior can be improved by an awareness workshop. The weak spots, which were filtered out were the willingness to share knowledge, the willingness of being a role model, the rejection of BYOD and the enthusiastic meaning about MDM. It has to be mentioned, that the main weakness of phase one is, that only weaknesses, which were discussed during the interview can be filtered out. Furthermore, another weakness of this proceed is, that it is based on several survey methods but also on subjective perception, so that another author could come (perhaps) to different assumptions about the weak spots of the security executives. To solve these problems, it would be necessary, to create a longer guideline with more questions about more issues and subjects. Certainly, the problem of subjective perception is always given and nearly impossible to eliminate completely.

The second phase was an awareness workshop that treaded four subjects, filtered from the weak spots of the experts: "Motivation", "Recognition", "BYOD" and "EMM". With the combination of basic knowledge, specific training and realistic examples, the awareness of every expert should be increased. Special attention was paid to the examples, because BYOD was seen very negative and MDM was seen very positive by the experts. Those examples serve to curtail their enthusiasm and to raise their awareness for alternative approaches. It should be also critical noted, that the amount of four different subjects is very small. Certainly, every phase needed exact and precise preparation, so that only selected topics could be discussed in an appropriate rate. A larger scale of workshops means also a cutback of the intensity of the training, which might have been a negative impact on the obtained results. However, a smaller workshop with a limited number of subjects, guarantees a more intensive learning process.

The impact of the workshops and the learning success was measured during the third phase of the awareness campaign. An online survey was created, that checked the learning progress of every expert. The evaluated results of the online survey showed that "Motivation", "EMM" and "Recognition" are important topics for the security executives, while BYOD is still no alternative approach for them. A reason for that could be that the used arguments in the BYOD workshop were not convincingly enough. Perhaps, it would be necessary to show more and even better researched ways to deal with the issue of BYOD. Otherwise, it could also be hopeless to convince german security executives of BYOD. That is why further research is needed to understand the total rejection of BYOD. Another limitation of the third phase is the short time period between phase two and three. For more accurate results, every expert could need more time to test his new skills during a working day. Furthermore, a longer time period would ensure that the experts had more time to reflect everything from the workshop. This could maybe have a positive influence on the obtained results. Besides, just a continuous repetition and improvement, of all three phases could lead to a lasting success

6 Conclusion and Outlook

This paper tries to answer the question, whether an awareness campaign designed for security executives, is able to affect their behavior and to make them aware of their personal deficits in regard to mobile security. To achieve this goal, an awareness campaign was created, based on theoretical and practical assumptions. Those essentials were used to design an own awareness campaign, which was also realized and evaluated during the practical part of this paper. The campaign was divided into three phases; each of them indispensable for success. The interviews, the workshop and the evaluation were created by significant standards, which were guaranteed by the fact that all important characteristics and components like "Identification of different types of employees", "Procure basic knowledge" or "Measurement of changed behavior" were integrated into the campaign. For that reason, the implementation was considerably easier and it was possible to complete all three phases of the campaign without restrictions. The evaluation of all contained information showed that all participated security executives gained their personal level of awareness. While before nearly all experts were not aware of sharing knowledge and the importance of being a role model, they do share their knowledge now with other employees and do accept the concept of mutual motivation. Furthermore, another important lesson learned from the awareness campaign was, that there is always room for improvement. No security concept is 100% proof and state of the art for all time and the same goes for the user. There is always room for self-improvement, which has to be an ongoing process that includes gaining knowledge about mobile security. Next to this, it has become evident, that security executives are the ideal target for awareness campaigns. In view of the fact, that a lot of stunning and interesting results were obtained, it can be suggested that this awareness campaign is a huge success. In future, it should be taken more care of longer time periods between the beginning of each phase, a more detailed survey and a continuous reputation of every phase to improve the effect of learning. These improvements are totally necessary, because awareness is a subject that will become even more important in future. This assumption is based on the fact that in future the number of mobile devices will increase rapidly, which could have the consequence that the percental amount of digital business issues will rise even faster than today. Today, aware employees are one of the most important keys to success. Without aware employees, an enterprise will not be able to stay in the market for very long. But, the research of this paper has proven, that even small campaigns with minor advices have a huge impact on someone's behavior. It is important to make every employee aware of the extent of damage, a wrong handling of a mobile device can cause. Without a good strategy and a well planed concept, it is nearly impossible to cope with all those new challenges and to provide knowledge where it is needed. Only when each employee is aware of the potential danger and the correct handling of mobile device, every technical security measure will work out. Without this kind of awareness, no system could become as prove as it had to be. Unfortunately, even today the percentage of human aspects in regard to mobile security is often underestimated. For that reason, it will be necessary to have a continuous improvement of several awareness concepts so that in future awareness campaigns will, just like technical measures, become a standard in every enterprise.

References

ALHARTHY K./ SHWAKAT W. (2013). IEEE International Conference on Control System, Computing and Engineering 2013, Implement Network Security Control Solutions in BYOD Environment, pp. 7-11

AVOLIO B. J./ LUFTHANS F./ WALUMBWA F. O. (2004). Authentic Leadership: Theory building for veritable sustained performance