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

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M.Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Ammann [redacted] [redacted] Vorname: Mathias [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 23.09.2014

Table of Content

1. Introduction

This Master's thesis was written during the summer term in 2014 at the Institute of Information Systems of the University of Hanover and serves the purpose to obtain the academic degree of Master of Science (M.Sc.).

1.1 Motivation and relevance

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.[1] Back at this time just less people were thinking about the issue of mobile security.[2] Even in the 1980s mobile devices like laptops or Notebooks, had the potential to cause several security problems for an enterprise, but back then, the number of laptops was very small and so the relevance of this topic.[3] Today the amount of 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, tablet-computer or laptop 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-Computers 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-computers to 221.3 million devices. A prediction from 2013 says that just four years later, 1685.8 million smartphones and 386.3 million tablet-Computers could be sold.[4] 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. This is the reason why companies try to protect their information systems by several security

[1] Cp. Weiser (1991) pp. 19-25
[2] Cp. Weiser (1991) pp. 19-25
[3] Cp. Scheepers et al. (2002) p. 1
[4] Cp. Statista (2014)

measures; but they also have to make sure, that all employees act safely.[5] Because of a rapidly increasing currentness and the fact that today nearly everyone is related to this topic, make *awareness* for a safe handling of mobile devices, such an important issue

1.2 Dissociation of the subject

What does awareness mean at this point? The term awareness evokes many things, which are not related to the issue of information security and mobile devices. Therefore, it is necessary to dissociate the subject, the paper is dealing with. This kind of prior demarcation makes it a lot easier to identify relevant issues later. Furthermore, it ensures that non essential subjects are not in focus, and precludes the possibility that important issues go unnoticed or get forgotten.

At first it is necessary to dissociate the term awareness. In this paper, the term awareness has a direct connection to the issue of mobile security, information systems like mobile devices and the leadership of executives. It has nothing to do with marketing, neuroscience or anything else. However, there is a need to specify the term awareness a little bit more. This paper is about designing and evaluating an awareness campaign for Information Security Executives in enterprises only. Employees, who have not a profession which comes close to a Security Executive, are not in focus of this survey. The principal focus of an enterprise is on security solutions, to ensure a better protection of sensitive data. Certainly this paper waivers a closer look to encryption or the programming of software and malware. The awareness campaign itself, should be in focus. Furthermore, term like *Mobile Device Management, Bring your own device*, *Mobile device* and *Smartphone* are in focus of this paper; even if they are not in the title itself. But these are essentials which are necessary for a better understanding of the empirical research.

Summarized, the objective of this paper is to show the reason, why Information Security Executives should pay more attention to the issue of mobile security. Most employees do

[5] Cp. Dagon et al. (2004) pp. 11-13

not draw attention to this issue, although they are using their mobile devices daily. For this reason it is necessary to show employees potential risks and make them aware for the issue of mobile security by showing them, how to act more safely with the support of an awareness campaign.

1.3 Structure of the Paper

For a better overview and to get structure in the amount of obtained information, it is important to explain the conduct of this paper. The first chapter starts with a short overview about the reason why awareness is an important issue for a safe handling of mobile devices. It is followed by the structure of the paper and ends with the derivation of several research questions. It shows the reason, why this paper was written, and why awareness is such an important issue. The second chapter covers the research design. It starts with a description, on which way relevant literature was identified and used. It gives an overview, why some papers were used for the research and why others were not. The second part of this chapter deals with the description of an interviewing process. This covers a short specification of the term "expert", a description of the process of a guided interview and an overview about several analyzing methods. It is followed by the third chapter, which is about the classification of abstract terms. This is necessary to inform the reader about important terms, issues and essentials to ensure a better understanding of the subject. It includes terms like, *Smartphone*, *Bring your own device (BYOD)*, *Mobile Device Management (MDM) Awareness, Big-Five Personality Traits and Awareness Campaign*. These essentials are followed by the empirical part of the paper: the design and evaluation of a mobile security awareness campaign for Security Executives. This part comprises three phases, to come to a result. The first one is the creation and evaluation of an interview, to obtain information for the design of the second phase of the awareness campaign: the execution of an awareness workshop. The empirical work ends with the third phase: an online survey to check the effect of the awareness campaign on the Security Executives. The campaign is followed by a summarization of the results in graphics and table form. This is necessary to prove an impact (of the awareness campaign) on the Security Executives, and to display their changed behavior.

1.4 Derivation of research questions

In order to achieve good results with the accomplishment of an awareness campaign, it is indispensable to frame several research questions. This process requires reflection, reformulation and debating of the issue, and the necessity to understand the intention of the review.[6] This research questions will be answered at the end of this paper with the support of an empirical investigation.

With regard to mobile devices, enterprises are exposed to high risks like malware, which increase rapidly.[7] But not only technical aspects are important to enterprises; the human factor is often even more essential. This is the reason why a loss of a device is also a huge risk, enterprises have to deal with.[8] For that reason, the term awareness receives more and more attention every day. On the one hand, several studies like from the russian antivirus software developer Kaspersky Lab have shown, that security incidents of enterprises are often caused by malware.[9] On the other hand, different studies are concentrating their attention on the human factor.[10] 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. Those studies are elucidating the importance of an interaction between technology and human behavior. This raises several questions about the capabilities of an awareness campaign, to train employees, to act more safely, while dealing with sensitive data. The main question is: leads security training for Information Security Executives to some kind of chain reaction, which affects all employees to care much more about security problems and the safety handling of mobile devices? Is it necessary to train every employee separately, or has an awareness campaign no impact at all? To answer these questions, it is necessary to derivate several research questions, which should be answered during the process of research, done in chapter four. In regard to an

[6] Cp. Okoli et al. (2010) p. 16
[7] Cp. Sabeeh et al. (2011) p. 428
[8] Cp. Singh (2012) p. 3
[9] Cp. Sabeeh et al. (2011) p. 428
[10] Cp. Fox (2003) p. 677

important and extensive topic like awareness, at least three research questions are sufficient, because one or even two question cannot contain everything important:

Research question 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?

Research question 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, because of their lack of know-how about mobile security?

Research question 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 of an enterprise for a better understanding of data integrity and a safer handling of mobile devices?

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. Other realistic examples had might convinced the Security Executives more than e.g. the six steps of IBM. 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, which is not just a flash in the pan.

6. Conclusions 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, clarified in chapter 3. Those clarifications involve the most important technical and also human aspects of mobile security. The emphases of the clarification were Mobile Devices, Bring Your Own Device and Mobile Device Management, which are all technical aspects. This chapter also contains information about Awareness, Awareness Campaigns and the Big-Five Personality Traits, which are more related to the human aspects of mobile security. 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. But, as already mentioned there is always room for improvement. 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. Because of that; 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.