Development of an Information Security Awareness Program to Prevent Social Engineering Attacks on Employees

Masterarbeit

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

vorgelegt von

Name: Swart Vorname: Lea

[redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 27.03.2019

Contents

1. Introduction

1.1 Motivation

In recent years, companies have become reliant on information technologies and online technologies to perform and improve their business tasks and to remain competitive (Abawajy, 2014; Safa and von Solms, 2016). Organizations communicate via social networking sites, provide data and information through online channels, and allow their employees to use personal mobile devices, such as smartphones and laptops for business as well as private use (Garba et al., 2015a; Garba et al., 2015b; Krombholz et al., 2015). In addition to the positive benefits of this development for companies, including the increased mobility, productivity, and availability of their employees (Mahesh and Hooler, 2013; Olalere et al., 2015), the relevance of information security is also growing (Safa et al., 2015). With information being shared online or stored on personal devices, businesses lose control over their sensitive data and thus become more vulnerable to malicious attacks (Krombholz et al., 2015; Olalere et al., 2015). Since companies have improved their technological defenses in recent years, social engineers now concentrate on the weakest link in information security: the employees of an organization (Abraham and Chengalur-Smith, 2010; Mouton et al., 2014a). Regarding malicious attacks on the end users of a company, SE is known as a vital threat (Abraham and Chengaluar-Smith, 2010).

Social engineering attacks are based on the manipulation of individuals with the aim of inducing information to be shared (Krombholz et al., 2015). This approach is particularly successful because it relies on the exploitation of human vulnerabilities such as emotions (Ivaturi and Janczewski, 2011) or the natural inclinations to trust others (Greavu-Serban and Serban, 2014) and to help people in need (Ghafir et al., 2016). Furthermore, most people cannot estimate the value of information they willingly provide to third parties and thus are not aware of possible malicious misuses (Bezuidenhout et al., 2010). Due to the high vulnerability of individuals, attackers no longer prioritize hacking into a company's security system to gain access to important information and data (Mouton et al., 2014b). Instead, intruders exploit unsuspecting employees and influence them to release data and facilitate the entry to the targeted systems (Mouton et al., 2014b; Saleem and Hammoudeh, 2018). During this type of exploitation, attackers rely on persuasion strategies (Wright et al., 2014).

The ease by which social engineers utilize manipulation tactics can be clarified through describing two recent attacks on companies. The first attack occurred during the final months of 2018. Social engineers approached specific employee groups such as management assistants via email and requested gift cards as rewards for certain staff members. In the course of this financially motivated attack, offenders often pretended to be high-ranking employees of the targeted companies (Cidon, 2018). According to the *Bundesamt für Sicherheit in der Informationstechnik* (BSI)*,* another attack, called *Emotet*, targeted German companies as well as private citizens and public authorities (BSI, 2019a). *Emotet* is a malicious software distributed via email and supposedly sent by large companies such as

Deutsche Telekom AG. An example of such an attack is an email that informs the user about a new invoice. As soon as the user opens the attached file, the included malware is capable of changing settings and passwords and exporting data out of the victim's computer (Laufenburg, 2018). The devastating consequences of *Emotet* for German companies are clearly visible. For example, in a Bavarian hospital, the entire computer technology system failed for two weeks due to an attack (Laufenburg, 2018). The BSI has reported similar incidents in which *Emotet* has led to the breakdown of companies' IT infrastructure, resulting in losses into the millions (BSI, 2019b).

Due to the devastating consequences of SE attacks for companies and the vulnerability of employees, the question of possible protective measures arises. In this context, current research supports the relevance of employee education through ISA programs (e.g. Smith et al., 2013; Abawajy, 2014; Kumar et al., 2015; Saleem and Hammoudeh, 2018). Existing study results demonstrate the positive impacts of these programs on knowledge about such attacks (e.g. Smith et al., 2013; Abawajy, 2014), the ability to identify malicious attempts (e.g. Kumaraguru et al., 2007a; Yang et al., 2012), and the security behavior of individuals (e.g. Jansson and von Solms, 2013). Thus, awareness-raising training is capable of decreasing the susceptibility of users to SE attacks (Brody et al., 2012).

However, as noted by Bauer et al. (2017), no real consensus exists regarding the setup of ISA programs. A review of existing literature identifies several research areas in this field that concern the selection of a suitable delivery medium (e.g. Yang et al., 2012; Abawajy, 2014; Bullée et al., 2016), the definition of the target group (e.g. Wu et al., 2012; Greavu-Serban and Serban, 2014; Saleem and Hammoudeh, 2018), and the choice of relevant content (e.g. Hadnagy, 2011; Chitrey et al., 2012; Smith et al., 2013), among other topics. The diverse academic research, together with the growing threat of SE attacks on organizations, has led to the goal of the present work: the presentation of recommendations for the design of an SE awareness program that specifically addresses employees. To gain comprehensive insights into this design, no concentration on specific elements occurs; instead, the recommendations include the design and realization of SE awareness-raising programs in companies. Thus, the aim of the work also follows the request of Chan and Mubarak (2012, p. 30): "In the long run, future research should also focus on including information security awareness as a part of an overall organizational security strategy by adopting suitable awareness enhancing programs."

To achieve the goal of the work, recommendations for the setup of ISA programs from the literature as well as based on practical experiences are compared, and further recommendations are generated. Furthermore, organizational factors supporting the realization of ISA programs in companies are identified. The chosen approach makes it possible to develop recommendations of particular relevance for an awareness program within a company. A quite similar approach has already successfully been applied by Bauer et al. (2017). However, the authors focus specifically on the structural and communicational elements of such programs and derived propositions of particular relevance for policy compliance in banks, whereas this paper focuses on the prevention of SE.

1.2 Research Question and Structure

The aim of the thesis is to answer the following research question:

How should an information security awareness program be designed to prevent social engineering attacks on employees?

To answer this question, this paper follows a certain structure (see Figure 1). The following chapter provides the theoretical foundation of the topic. First, it offers definitions of SE and introduces a comprehensive SE taxonomy to fully capture this specific attack approach. Furthermore, it explains the vulnerabilities of individuals towards social attacks and addresses the manipulation tactics used by social engineers to attack target victims. The treatment of these two issues is particularly important to develop a first understanding of the need for prevention measures against SE. The final part of Chapter 2 addresses the relevance of ISA programs. In this passage, the security awareness and behavior of employees is described with the help of different behavioral theories, and the effectiveness of ISA programs on the information security of organizations is highlighted.

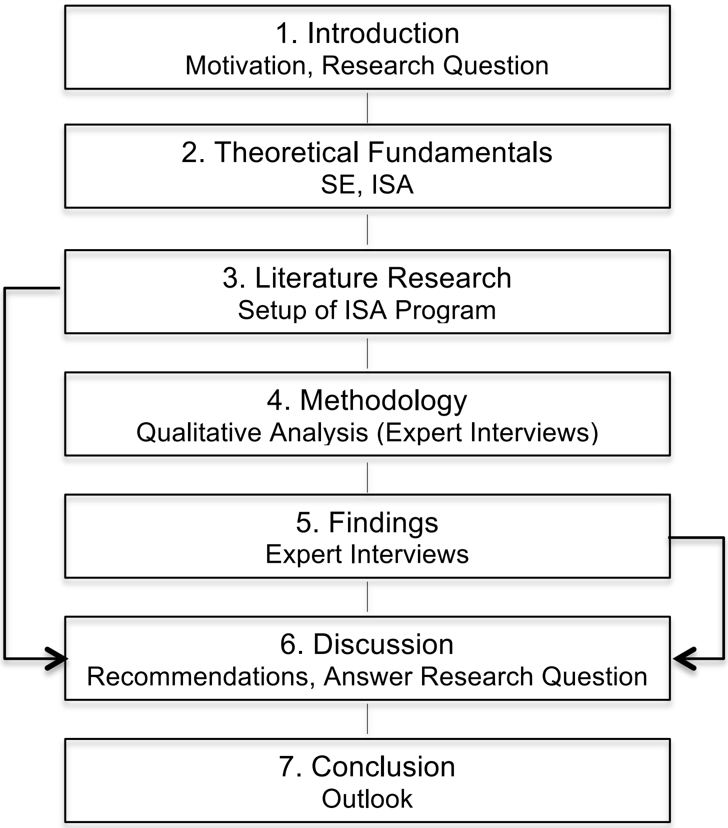

Figure 1 Structure of Thesis (own illustration)

As illustrated in Figure 1, the answer to the research question is based on a literature review as well as expert interviews. This approach allows the comparison of practical and theoretical insights concerning the setup of awareness trainings and thus enables the deduction of recommendations concerning SE awareness programs. The literature review, contained in Chapter 3, introduces the primary concepts of ISA programs and offers recommendations based on academic research on this topic. This review represents the current best practices.

Chapter 4 subsequently describes the qualitative method of expert interviews, which are used to generate practical insights in addition to the academic-based views. Chapter 5 presents the results of the conducted interviews. The discussion in Chapter 6 compares the outcomes from Chapter 3 and Chapter 5 and derives recommendations. As result of the discussion, an overview of recommendations that contribute to the development of an SE awareness program is presented. Furthermore, implications for research and practice as well as the limitations of the paper are introduced. The paper ends with a conclusion.

7. Conclusion

Today, many companies face the risk of security breaches and resulting data losses due to SE attacks. Since social attacks rely on manipulation techniques with the aim of exploiting human weaknesses, employees are a weak point in the information security of organizations. Therefore, the implementation of ISA programs in companies as protective measures to secure employees against SE attacks is particularly relevant. As such, this thesis aimed to deduce recommendations concerning the development of an ISA program to prevent SE attacks on employees. Based on the research objective, the work provides theoretical insights regarding the subjects of SE and ISA. Building on this, a comprehensive literature review on awareness programs was conducted. With the help of the approach of Webster and Watson (2002), six broad concepts were identified that are relevant for the setup and realization of SE awareness programs. Furthermore, the primary portion of the work was the qualitative approach of expert interviews. This method was chosen to gain insights into the practical implementation of SE awareness programs in an organizational context. Based on the interpretation and the discussion of interview findings with regard to the literature results, the work provides 21 recommendations concerning the design and implementation of an SE awareness program for employees.

The thesis has answered the research question “How should an information security awareness program be designed to prevent social engineering attacks on employees?” in such a manner that no generally valid solution suitable for all companies is identified. Rather, the program should be customized to the individual characteristics and needs of an organization and its employees. Nevertheless, the deduced recommendations provide valuable insights regarding the content, delivery media, user friendliness, attack simulation, regularity, target group, and even intra-organizational requirements of SE awareness programs. For each of the components, several recommendations are presented that should be considered in theory as well as in practice. Particularly important are the contributions of the expert interviews to the contrasting opinions in academic research with regard to the target group and the different delivery methods.

Overall, the results of the thesis offer different research directions for the future. Further research is necessary in the field of attack simulations, namely the execution of physical attack simulations with a broad target group as well as the pre-announcement of simulations in the organization. Furthermore, another interesting aspect for future studies would be the development of an SE awareness program that focuses in particular on young users and the review of its effectiveness. Last but not least, new academic insights regarding the positive handling of employees’ security-related mistakes and its impact on their likelihood to report security breaches are necessary. This research is particularly important for the organizational context, as it could provides insights into how to shape a positive employee culture in dealing with security faults.

In conclusion, it is necessary to emphasize the already high and ever-increasing danger of SE attacks on companies: “This is certainly the topic of the future because it cannot be completely prevented on a technical basis” (E-SEC GmbH, p. 92). This expert statement reflects the opinion of almost all interviewed practitioners, as well as academic researchers (e.g. Aloul, 2012; Kumar et al., 2015; Saleem and Hammoudeh, 2018), that organizations must focus on protection against social attacks, making the education of employees even more critical in the future.