SOCIAL ENGINEERING AND INFORMATION AND COMMUNICATION TECHNOLOGIES

António Lopes[1]
Leonilde Reis[2]

DOI: https://doi.org/10.31410/LIMEN.2020.185

Abstract: *Social Engineering, in view of the current dependence of information systems and information and communication technologies organizations, is of great interest in creating conditions, in order to reduce the threats and vulnerabilities, to which organizations are exposed. Thus, Social Engineering is considered to have emerged as a serious threat in virtual communities and is an effective way of attacking information systems, by creating conditions in order to jeopardize business continuity. The article presents the problem in the field of Information Security, emphasizing concerns in the field of Social Engineering in view of the vulnerabilities to which the generality of organizations is exposed. The research methodology adopted is Design Science Research, given the specificity of the problem. The main results are the literature review in the field of Social Engineering, with special emphasis on attack models and a reflection of the real-world professional experience.*

Keywords: *Social engineering, Information security, Information systems, Information and communication technologies.*

INTRODUCTION

Currently, the majority of organizations are dependent on their Information Systems (IS), supported by the Information and Communication Technologies (ICT). It is considered that this interdependency is often scaled up and organizations are exposed to various vulnerabilities.

Therefore, the problem surrounding the issues concerning Information Security (InfoSec), is of particular interest, namely Social Engineering. It is considered that the services used by the organizations stakeholders enhance the preparation of spaces for sophisticated attacks of Social Engineering (ES).

The analysis of the national legal framework and relevant international regulations/standards in this field may be of interest in the sense of systematizing knowledge. It is considered that the analysis of ISO/IEC 27001:2013, ISO/IEC 27002:2013 and ISO/IEC 27008:2019 standards may constitute added value in identifying components to be included in a Framework, in which the social engineering problem is systematized.

The *Design Science Research* (DSR) methodology was adopted as a theoretical basis for sustaining the scientific validity for the elaboration of this work (Peffers, Tuunanen, Rothenberger, & Cha, 2007). Because it is a research methodology indicated for research projects in technologies and information systems and systems architectures, (Ferreira, Ferreira,

[1] Polytechnic Institute of Setúbal, Portugal
[2] Polytechnic Institute of Setúbal, Portugal

Silva, & Carvalho, 2012), inherent to the activity design ensures in this way, discipline, rigor and transparency, (Pedro, 2015), cited by, (Lacerda, Dresch, Proença, & Antunes Júnior, 2013). It is a widely used methodology in the domain of IS because it has the necessary iterations for the development of the artifact, in order to be possible to define a framework.

SOCIAL ENGINEERING

Is considered that ES has emerged as a serious threat in virtual communities and is an effective means of attacking IS. The services used by employees enhance the preparation of spaces for sophisticated ES attacks. The growing trend towards Bring Your Own Device (BYOD) policies and the use of online communication and collaboration tools in private and business environments worsen the problem (Krombholz, Hobel, Huber, & Weippl, 2015). An ES attack aims to exploit vulnerabilities using various manipulation techniques to obtain sensitive information. ES's dominance is still in the early stages, regarding formal definitions, attack frames and attack models (Mouton, Leenen, & Venter, 2016).

ES attack models generally cover the three types of communication, namely two-way communication, one-way communication, and indirect communication. To perform comparative studies of different models, processes and frameworks, it is necessary to have a formalized set of scenarios of ES attacks that are fully detailed in all phases and stages of the process. ES attack models are converted to ES attack scenarios, populating the model with individuals and objects from real-world examples, maintaining the detailed flow of the attack, as provided in the model, (Mouton, Leenen, & Venter, 2016).

Decreased personal interaction combined with a multitude of tools used for communication *(email, IM, Skype, Dropbox, LinkedIn, Lync,* etc.) create new attack vectors for ES attacks. Attacks on companies show that targeted phishing *attacks* are an effective and evolving step in ES attacks that constitute a dangerous weapon that is often used by advanced persistent threats (Krombholz, Hobel, Huber, & Weippl, 2015).

A *phishing* attempt is an example of an attack ES. As in a banking institution or other organization where you have an account, ES uses this method and may use company logos or information about you to appear as a legitimate user (Srivastava, Walker, & Olson, 2015).

Semantic attacks are the specific type of ES attacks that mislead technical defenses by actively manipulating the characteristics of objects, such as platform or system applications, to trick rather than directly attack the user. Generally observed examples include URL's, phishing emails, drive-by downloads, fake websites and scareware (Heartfield & Loukas, 2015).

It is considered that the methods and systems of ES attack deployment include: extracting one or more non-semantic data items from an incoming e-mail; determine whether non-semantic data correspond to the information stored in a previously collected information database; conducting behavioral analyses on one or more items of non-semantic data; analyzing semantic data associated with e-mail to determine whether non-semantic data corresponds to one or more patterns associated with malicious emails; and based on determination, realization and analysis, identifying email as potentially malicious or non-malicious, may constitute added value, (Srivastava, Walker, & Olson, 2015).

SOCIAL ENGINEERING ATTACK MODELS

Current studies aim to demonstrate the usefulness of ES Attack Frameworks in preventing ES attacks. One of these studies, released by (Mouton, Leenen, & Venter, 2016), states that when a question is posed to the potential victim of attack, it is very important that they identify, without any doubt, what information is being requested.

Figure 1. Social Engineering Attack Deployment Model

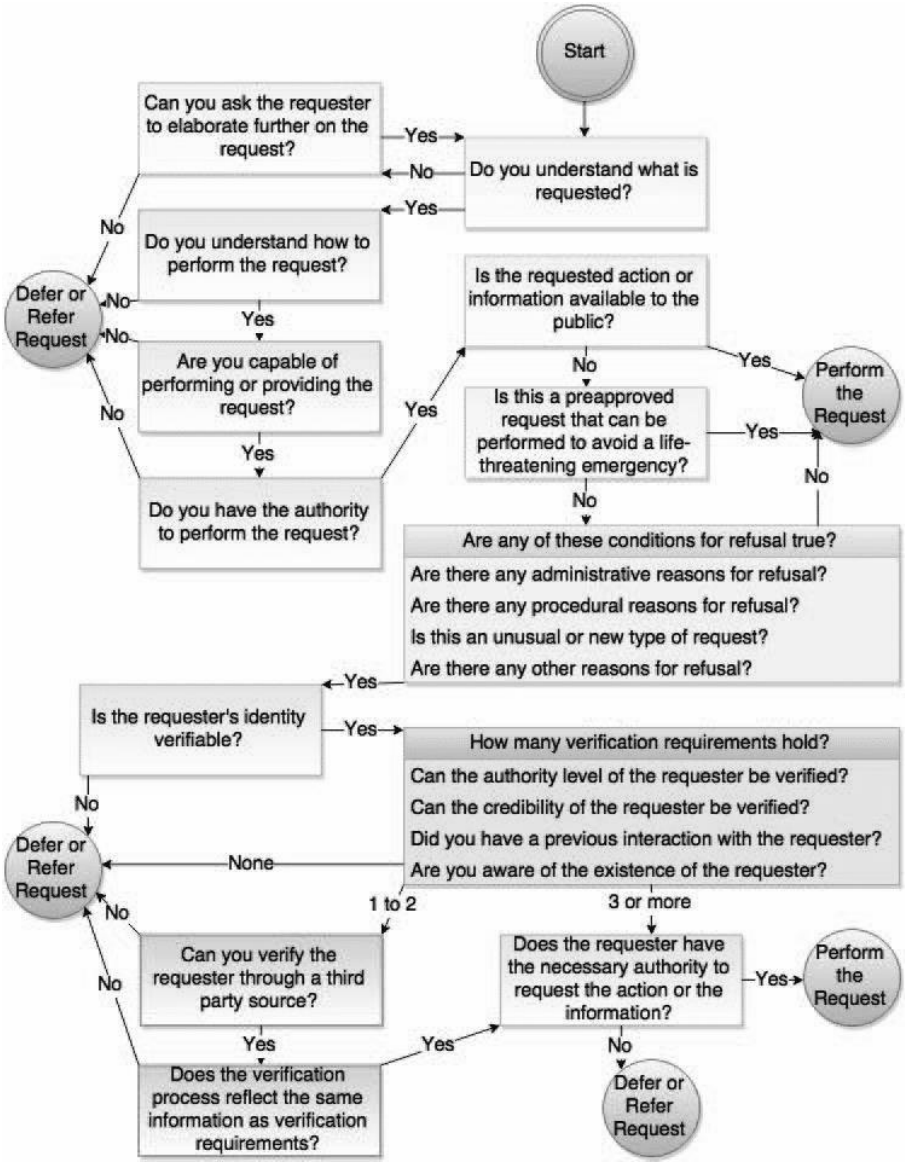

Figure 1 presents a proposed model in order to identify the possibility of facing an Attack of ES. In view of the study carried out, it is emphasized that the Framework is in the initial phase of development. The Framework will be multidisciplinary and aggregator of international standards, legal framework, recommendations, guiding and supporting stakeholders in the selection and definition of controls that ensure the security of organizational information and avoid possible attacks of Social Engineering. The framework under development has the objective to incorporate the valences underlying the scientific vision under study in the field of theme, but also the organizational practices defined as well as incorporate the practical know-how obtained in the international context.

FUTURE RESEARCH DIRECTIONS

As ICT evolves, ES attacks become increasingly frequent. It is also considered imperative to include, in this context, the sustainability concerns of ICT, (Silveira & Reis, 2020) and (Reis, et al. 2020). In this sense, ES is able to implement strategies for manipulating people's minds to obtain private information, instead of attempting the attack on security devices. It is advocated that a set of strategies should be delineated, so that people are aware of the problems of InfoSec, namely likely attacks of ES.

In view of the studies analyzed, it is also concluded that most incidents with InfoSec are related to processes and human behavior itself, to the detriment of more technical issues. The prospects for future work are intended to continue the development of the Framework within the InfoSec Framework, more specifically in the area of ES, which allows the understanding and integration of issues related to ES, in order to allow the definition of strategies (Lopes & Reis, 2021).

CONCLUSION

It is considered that in view of the increasing dependence on ICT businesses, organizations are generally vulnerable in the field of InfoSec. In this sense, and face to the studies analyzed, it is also concluded that most incidents with InfoSec are related to processes and human behavior itself, rather than technical issues.

Regardless the importance and pertinence of the development of a multidisciplinary framework and aggregator of a set of valences, it has the intention of contributing to brist gaps in this field of knowledge.

The future work perspectives are intended to continue the development of the Framework within the InfoSec field, more specifically in the area of ES, which allows understanding and integrating issues related to ES, helping in the definition of strategies and optimizing the practices currently established in organizations.

REFERENCES

Bianchi, I., & Dinis de Sousa, R. (2015). Governança de TI em universidades públicas: Proposta de um modelo. Instituto Universitário de Lisboa (ISCTE-IUL). Obtained from http://hdl.handle.net/1822/39467

Eiras, M. (2004). Engenharia Social e Estelionato Eletrônico. Rio de Janeiro.

Ferreira, I., Ferreira, S., Silva, C., & Carvalho, J. (2012). Dilemas iniciais na investigação em TSI design science e design research, uma clarificação de conceitos. Proceedings of Conferência Ibérica de Sistemas y Tecnologias de Informação. Obtained from https://repositorium.sdum.uminho.pt/bitstream/1822/21696/1/CISTI 2012.pdf.

Heartfield, R., & Loukas, G. (December de 2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys(37). doi: https://doi.org/10.1145/2835375

Hevner, A., March , S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 1(28), 75–105.

ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements. ISO/IEC.

ISO/IEC 27002:2013. (2013). Information technology — Security techniques — Code of practice for information security controls. ISO/IEC.

ISO/IEC 27008:2019. (2019). Information technology — Security techniques — Guidelines for the assessment of information security controls. ISO/IEC.

Kaspersky. (2020). What is Social Engineering?: Obtained from https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (June de 2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122. doi:https://doi.org/10.1016/j.jisa.2014.09.005

Lacerda, D. P., Dresch, A., Proença, A., & Antunes Júnior, J. A. (2013). Lacerda, D. P., Dresch, A., Proença, A., & Antunes Júnior, J. A. V. (2013). Design Science Research: 89 método de pesquisa para a engenharia de produção. Gestão & Produção, 20(4),. pp. 741–761. Obtained from Design Science Research: método de pesquisa para a engenharia de produção. Gestão & Produção, 20(4), 741–761,: https://doi.org/10.1590/S0104-530X2013005000014

Lopes, A. & Reis, L. (2021). Framework para avaliação de ameaças à segurança de informação com recurso a engenharia social no contexto organizacional. V International Forum on Management. Instituto Politécnico de Setúbal. Setúbal.

Mitnick, K. D., & Simon, W. L. (2003). A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education.

Mouton, F., Leenen, L., & Venter, H. (June de 2016). Social Engineering Attack Examples, Templates and Scenarios. Elsevier Computers & Security, 59, 186-209. doi:https://doi.org/10.1016/j.cose.2016.03.004

Mouton, F., Leenen, L., & Venter, H. S. (2015). Social Engineering Attack Detection Model: SEADMv2. International Conference on Cyberworlds (CW), pp. 216-223.

Mouton, F., Leenen, L., Malan, M., & Venter, H. (2014). Towards an Ontological Model Defining the Social Engineering Domain, in Kimppa, K. et al. (eds) ICT and Society . (S. B. Heidelberg, Ed.) IFIP Advances in Information and Communication Technology, 266-279. doi:https://doi.org/10.1007/978-3-662-44208-1_22

Pais, R., Moreira, F., & Varajão, J. (2013). Engenharia Social (ou o carneiro que afinal era um lobo). doi:http://hdl.handle.net/11328/1347

Pedro, S. (2015). Modelação de Processos para as principais áreas de Recursos Humanos. Nova Information Management School.

Peffers, K., Tuunanen, T., Rothenberger, M., & Cha. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 3(24), 45-78.

Reis, L., Silveira, C., Péricles, C., Pires, G., Carvalho, L., & Mata, C. (2020). The potential of technology in transforming it into a more sustainable society model – The Homeless Person case. 20ª Conferência da Associação Portuguesa de Sistemas de Informação - CAPSI 2020. Porto, Portugal.

Russo, N., & Reis, L. (2020a). Certificação de Programas de Faturação - Guia para a Continuidade de Negócio. Lisboa: FCA.

Russo N., & Reis, L., (2020b). Methodological approach to systematization of Business Continuity in organizations, in L. Cagica Carvalho, L. Reis, A. Prata, R. Pereira (eds), Multidisciplinary Approach to Entrepreneurship, Innovation, and ICTs, USA: IGI Global.

Roquete, M. (2018). Modelo de maturidade para apoio à implementação de uma filosofia de gestão orientada a processos numa organização. Nova Information Management School, Lisboa.

Sêmola, M. (2014). Gestão da segurança da informação: Uma Visão Executiva (2ª ed.). São Paulo: Elsevier.

Silveira, C. & Reis, L., (2020). Sustainability in Information and Communication Technologies, in L. Cagica Carvalho, L. Reis, A. Prata, R. Pereira (eds), Multidisciplinary Approach to Entrepreneurship, Innovation, and ICTs, USA: IGI Global.

Srivastava, M., Walker, W., & Olson, E. (2015). Social Engineering Protection. QINETIQ North America, Inc.

Thornburgh, T. (October de 2004). Social engineering: the "Dark Art". InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development, (pp. 133-135). doi:https://doi.org/10.1145/1059524.1059554