Presentation the interaction of the subject and the object of socio-engineering influence with a social graph

Tsurkan Oksana[1]
[1]Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, otsurkan24@gmail.com

Herasymov Rostyslav[2]
[2]Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, gerasimov.rostislav@gmail.com

Kruk Olha[3]
[3]Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, o.n.kruk@gmail.com

Abstract. *The use of social engineering as an interaction between an attacker and an employee is considered. It shows its focus on receiving sensitive information. This is achieved by an attacker by studying, engaging, trusting, using employee trust. To prevent this, psycho-personal qualities, professional competences of the social engineer and employee are taken into account, and their interaction is represented by a social graph. Its tops reflect a social engineer, employee, quality and compensation; connections – the relationship between them. This approach will make it impossible to manipulate the employee's mind.*

Keywords: *соціальна інженерія, соціальна взаємодія, маніпуляція, форми маніпуляції, соціальний граф.*

I. Introduction and Problem statement

The use of social engineering is reduced to the interaction of the attacker with an employee of the organization. Such interaction is focused on receiving confidential information and is implemented in four phases: studying, establishing interaction, entering into trust, using trust [1-3].

An example of the study of these phases is the social engineering optimizer. They are used by separating the attacker (social engineer) and protector (employee of the organization). Each is initialized by two random decisions. Better among them is interpreted as an attacker. To achieve this, he adheres to social engineering methods [4].

However, the consideration remains that during the interaction, the social engineer manipulates the employee's consciousness and, as a consequence, gains sensitive information.

II. Problem solution and Results

According to the socio-engineering approach the vulnerabilities of the employee are interpreted as his weaknesses, needs, mania (passions), admiration. This leads to a new model of his behavior, creating favorable conditions for the implementation of threats to the use of social engineering. The manifestation of such forms is fraud, deception, scam, intrigue, hoax, provocation. The social engineer intentionally influences the employee's mind against will, but with his or her consent.

Therefore, it is important to take into account their psychological and personal qualities and professional competences when interacting.

In order to take into account the psychological and personal qualities, professional competencies of the social engineer and the employee of the organization, it is recommended that their interaction be represented by a social graph [5, 6].

Social graph represents the interaction of the subject (social engineer) with the object (employee of the organization) of socio-engineering influence and the connection between them

$$G = (V, E),$$

where G – social graph; V – set of peaks (e.g., social engineer, employee, software tool, psychological and personal qualities, professional competences); E – set of connections (e.g., "social engineer – employee", "social engineer – software tool", "employee – software tool", "employee – qualities").

III. Conclusions

Thus, the use of social engineering is reduced to manipulating the attacker with the employee's mind against the will, but with his or her consent. To prevent this, the psycho-personal qualities, professional competencies of the subject and the object of such interaction are taken into account by presenting them with a social graph.

References

[1] O. Tsurkan, R. Herasymov, and O. Kruk, "Methods of counteracting social engineering", Information Technology and Security, vol. 7., iss. 2 (13), pp. 161-170, July-December 2019, doi: 10.20535/2411-1031.2019.7.2.190563.

[2] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186-209, September 2016, doi: 10.1016/j.cose.2016.03.004.

[3] S. Ellis, "Social Engineering Deceptions and Defenses", in Computer and Information Security Handbook, J. Vassa, Eds. Burlington, USA: Morgan Kaufmann, 2017, pp. 465-474, doi: 10.1016/B978-0-12-803843-7.00029-6.

[4] A. Fathollahi-Fard, M. Hajiaghaei-Keshteli, and R. Tavakkoli-Moghaddam, "The Social Engineering Optimizer (SEO)", Engineering applications of artificial intelligence, vol. 72, pp. 267-293, June 2018, doi:10.1016/j.engappai.2018.04.009.

[5] V.V. Mokhor, O.V. Tsurkan, R.P. Herasymov, and V.V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering Approach", Selected Papers of the XVII International Scientific and Practical Conference "Information Technologies and Security". Kyiv, 2017. pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol2067/paper13.pdf.

[6] J. Gross, J. Yellen, and M. Anderson, Graph theory and its applications. Boca Raton, USA: CRC Press, 2019.