Analysis of Social Engineering in an Organization with prevention strategies

INTRODUCTION

In this information age, the internet has become a part of our daily lives, resulting in an increase in cyber-attacks with social engineering at the forefront. The psychological manipulation of the user to obtain sensitive information for malicious purposes is known as social engineering. Because social engineering attacks are based on humans rather than software, they are difficult to prevent. They can take many forms as they involve human interaction. Several organizations have suffered significant losses as a result of social engineering attacks. A loss of $121.22 billion is estimated to have occurred as a result of social engineering [1]. Social engineering attacks will become a greater threat as technology advances, necessitating immediate attention [2]. This review examines social engineering, types of attacks, examples, and methods of attack, particularly in an organization, and offers potential countermeasures. This review consists of types of social engineering, a case of social engineering, social engineering framework, and mitigation for social engineering.

Keywords: social engineering, attacks, organizations, mechanisms, phishing, tailgating, mitigation

DISCUSSION

An organization is defined as a network of people, assets, and processes which interact with one another in defined roles and functions towards a common goal [3]. In an organization, social engineering attacks rely on employees ' individual characteristics to steal information rather than relying on standard technology shortcomings to gain access to data [4]. They exploit human weaknesses such as carelessness and ignorance, making attacks difficult to prevent. Purushotham and Gowthamaraj [5] argue that with technology constantly advancing and attacks taking different forms, social engineering cannot be fully prevented. Over time, it has become the biggest cyber threat faced by an organization. Among the many forms of social engineering, the most common are tailgating and phishing. Tailgating involves creating a character and inventing a fake story to utilize the employee's basic emotions. It entails accompanying an employee with authorized access into a restricted area [6]. It could be as simple as convincing the employee he has forgotten or lost his ID card**.** Phishing is one of the predominant methods utilized to extract data [7]. It involves sending fake emails to get the employee to click on a fake website. The individuals are then tricked into filling out information or injecting malicious programs onto their PC [2].

One example of a phishing attack happened in 2016 when the Democratic National Convention suffered a social engineering attack during the United States election campaign. The social engineer simply sent an email with a link asking users to change passwords, and almost 19,000 emails were stolen and leaked from the email accounts belonging to the prominent members of Clinton’s campaign [7].

Although social engineering attacks take many forms, they adopt a basic common process [8]. Understanding how social engineering attacks succeed requires an understanding of the effect mechanism, human vulnerability, and attack method [9], and aids in developing mitigations to such attacks. Mike and Minhaz proposed three stages as the key to any social engineering attack [2]. Phase one is referred to as the attack formulation stage. The goal and target of the attack are identified. It could constitute a person or an organization. Phase two involves information gathering. This entails comprehensively obtaining information on individuals, an organization, and its employees, hours of operation, the organization's current security, and many more. Phase three refers to the attack phase. In this, the social engineer analyzes information obtained and employs one or more of the attack types to deal damage.

With the knowledge obtained from analyzing social engineering attack patterns, several solutions have been proffered over the years to counter social engineering, but with the ever-growing social engineering, several methods have proven ineffective. As previously stated, social engineering attacks target humans, whom H. Aldawood and G. Skinner identify as the weakest link in system security [10]. Essentially many people are unaware of social engineering and its operation. One prominent approach according to Hussain et al, to reduce social engineering attacks would be for organizations to offer adequate training to increase employees' security knowledge, as well as invest in raising employees' awareness of social engineering [4]. Employees who understand social engineering and how it operates will identify attack patterns and implement security practices that will effectively prevent social engineering attacks in organizations.

CONCLUSION

This review set out to analyze social engineering in organizations and proffer possible solutions for such attacks. Social engineering, as already established, involves the psychological manipulation of individuals to obtain information. Although Several solutions are recommended, the most effective prevention method is security awareness programs. Ignorance has been established as a major factor in social engineering attack success and raising awareness as well as informing employees about attack methods will actively deter such attacks. Factors such as social, economic, and cultural background affect how humans interact with technology. There is currently insufficient information on how the human mind operates in relation to technology and further study is recommended in this field.

REFERENCES

[1] F. Salahdine and N. Kaabouch, '*Social Engineering Attacks: A Survey*', Future Internet, vol. 11, no. 4, p. 89, Apr. 2019, DOI: 10.3390/fi11040089.

[2] M. Mattera and M. M. Chowdhury, '*Social Engineering: The Looming Threat*', in 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, May 2021, pp. 056–061. DOI: 10.1109/EIT51626.2021.9491884.

[3] H. Wilcox and M. Bhattacharya, '*A framework to mitigate social engineering through social media within the enterprise*', in 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), Hefei, China, Jun. 2016, pp. 1039–1044. DOI: 10.1109/ICIEA.2016.7603735.

[4] H. Aldawood, T. Alashoor, and G. Skinner, '*Does Awareness of Social Engineering Make Employees More Secure?*', IJCA, vol. 177, no. 38, pp. 45–49, Feb. 2020, DOI: 10.5120/ijca2020919891.

[5] P. P. Parthy and G. Rajendran, '*Identification and prevention of social engineering attacks on an enterprise*', in 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, Oct. 2019, pp. 1–5. DOI: 10.1109/CCST.2019.8888441.

[6] N. Duarte, N. Coelho, and T. Guarda, '*Social Engineering: The Art of Attacks*', in Advanced Research in Technologies, Information, Innovation, and Sustainability, vol. 1485, T. Guarda, F. Portela, and M. F. Santos, Eds. Cham: Springer International Publishing, 2021, pp. 474–483. DOI: 10.1007/978-3-030-90241-4_36.

[7] P. P. Parthy and G. Rajendran, '*Identification and prevention of social engineering attacks on an enterprise*', in 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, Oct. 2019, pp. 1–5. DOI: 10.1109/CCST.2019.8888441.

[8] S. A. D. T. P. Kaushalya, R. M. R. S. B. Randeniya, and A. D. S. Liyanage, '*An Overview of Social Engineering in the Context of Information Security*, in 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bangkok, Thailand, Nov. 2018, pp. 1–6. DOI: 10.1109/ICETAS.2018.8629126.

[9] Z. Wang, H. Zhu, and L. Sun, '*Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods'*, IEEE Access, vol. 9, pp. 11895–11910, 2021, DOI: 10.1109/ACCESS.2021.3051633.

[10] H. Aldawood and G. Skinner, '*Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*', in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Dec. 2018, pp. 62–68. DOI: 10.1109/TALE.2018.8615162.