Topic ID: 324-IT-EN

Detection of Social Engineering in Cyberspace Threats

Supervisor: Prof. Ing. Komínková Oplatková Zuzana, Ph.D.

Consultant: Ing. Malaník David, Ph.D., ---

Department: Department of Informatics and Artificial Intelligence

Programme: Information Technologies

Abstract:

Elements of social engineering can be observed in all attacks we encounter in cyberspace today. Attackers have already understood that using these techniques significantly increases the probability of success. As threats on the Internet have evolved, social engineering techniques have evolved and improved at the same time. Thus, the tried ways of detecting a sociotechnical attack often do not apply. Attackers know about them too and seek ways to exploit other opportunities and the gullibility of victims, who often stick to these methods. Unfortunately, as the success rate of sociotechnical attacks increases, the success rate of catching attackers decreases. This is because it is often more difficult to get relevant data about an incident from a person (the victim) than from computers and network elements.

The topic of this thesis traces the developments and trends in the field of social engineering in relation to attacks in recent years. The focus is on finding or evaluating trends and general signatures used by social engineers. The thesis also envisages the use of artificial intelligence and available technologies of large language models, such as ChatGPT, for the implementation of social engineering attacks. In the context of investigating actual attacks, an integral part is to research and determine the possibilities of detecting these attacks based on some advanced methods, e.g., using artificial intelligence (AI) and deep learning (DL).

The research objective is to find, classify and describe possible attacks using social engineering and to propose effective countermeasures applicable in real life operations.

Literature:

[1] HADNAGY, Christopher. Social engineering: the science of human hacking. Second edition. Indianapolis, IN: Wiley, [2018], xxii, 297 s. ISBN 978-1-119-43338-5.PINEDO, Michael L., 2016. Scheduling: Theory, Algorithms, and Systems. 5th ed. 2016 edition. Cham Heidelberg New York Dordrecht London: Springer. ISBN 978-3-319-26578-0.

[2] EVANS, Lester. Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners. [USA]: [Lester Evans], [2019], 218 s. ISBN 9781794647237.DETTI, Paolo, 2018. Production And Supply Chain Management - Logistics. LAMED - Decision Methods Laboratory [online]. Dostupné z: http://www.dii.unisi.it/~detti/GestProdSupChain.htm

[3] Arun Vishwanath, "THE WEAKEST LINK," in The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing , MIT Press, 2022, pp.1-6.

[4] MONTANẼZ RODRIGUEZ, Rosana, Shouhuai XU, Gerhard GOOS, et al. Science of Cyber Security: 4th International Conference, SciSec 2022, Matsue, Japan, August 10–12, 2022, Revised Selected Papers. 13580. 2022, 487-504. ISBN 9783031175503. Online: doi:10.1007/978-3-031-17551-0_32.

[5] MASHTALYAR, Nikol, Uwera Nina NTAGANZWA, Thales SANTOS, et al. Social Engineering Attacks: Recent Advances and Challenges. HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings [online]. 2021, 12788, 417-431 [cit. 2023-07-03]. ISBN 9783030773915. ISSN 03029743. Online: doi:10.1007/978-3-030-77392-2_27.

[6] YASER AL-BUSTANI, Abdulateef M., Abdul Karim ALMUTAIRI, Abdullah ALRASHED a Abdul Wahab MUZAFFAR. Social Engineering via Personality Psychology - Bypassing Users Based on Their Personality Pattern To Raise Security Awareness. 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), IT Innovation and Knowledge Discovery (ITIKD), 2023 International Conference on [online]. 2023, 1-8 [cit. 2023-07-03]. ISBN 9781665463720. ISSN edseee.IEEEConferenc. Online: doi:10.1109/ITIKD56332.2023.10100048.

[7] TAIB, Ronnie, Kun YU, Shlomo BERKOVSKY, et al. Human-Computer Interaction – INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part I. 11746. 2019, 564-584. ISBN 9783030293802. Online: doi:10.1007/978-3-030-29381-9_35.

[8] GRBIC, Dijana Vukovic a Igor DUJLOVIC. Social engineering with ChatGPT. 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH), INFOTEH-JAHORINA (INFOTEH), 2023 22nd International Symposium [online]. 2023, 1-5 [cit. 2023-07-03]. ISBN 9781665475457. ISSN 27679470. Online: doi:10.1109/INFOTEH57020.2023.10094141.

[9] SALAMA, R., F. AL-TURJMAN, S. BHATLA a S.P. YADAV. Social engineering attack types and prevention techniques- A survey. 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Computational Intelligence, Communication Technology and Networking (CICTN), 2023 International Conference on [online]. 2023, 817-820 [cit. 2023-07-03]. ISBN 9798350338027. ISSN edseee.IEEEConferenc. Online: doi:10.1109/CICTN57981.2023.10140957.

[10] DUMAN, S.A., R. HAYRAN a I. SOGUKPINAR. Impact Analysis and Performance Model of Social Engineering Techniques. 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Digital Forensics and Security (ISDFS), 2023 11th International Symposium on [online]. 2023, 1-6 [cit. 2023-07-03]. ISBN 9798350336986. ISSN edseee.IEEEConferenc. Online: doi:10.1109/ISDFS58141.2023.10131771