Kód tématu: 345-IT-CZ

Detekce sociálního inženýrství v hrozbách kyberprostoru

Školitel: prof. Ing. Komínková Oplatková Zuzana, Ph.D.

Konzultant: Ing. Malaník David, Ph.D., Ing. Žáček Petr, Ph.D.

Ústav fakulty: Ústav informatiky a umělé inteligence

Studijní program: Informační technologie

Anotace:

Prvky sociálního inženýrství lze v současné době pozorovat v podstatě u všech útoků, se kterými se v kyberprostoru setkáváme. Útočníci již dávno pochopili, že se s využitím těchto technik významným způsobem zvyšuje pravděpodobnost úspěchu. S vývojem hrozeb v síti Internet dochází současně i k vývoji a vylepšování technik sociálního inženýrství. Často tak neplatí zažité způsoby, jak detekovat sociotechnický útok. Útočníci o nich vědí a snaží se hledat cesty, jak využít dalších možností a důvěřivosti obětí, které se těchto způsobů často drží. Bohužel se stoupající úspěšností sociotechnických útoků klesá i úspěšnost dopadení útočníků. Z člověka (oběti) se totiž mnohdy relevantní data o daném incidentu dostávají obtížněji než z počítačů a síťových prvků.

Téma práce mapuje vývoj a trendy v oblasti sociálního inženýrství v návaznosti na útoky z posledních let. Důraz je kladen na nalezení, případně zhodnocení trendů a obecných signatur používaných sociálními inženýry. Práce počítá i s využitím umělé inteligence a dostupných technologií velkých jazykových modelů, např. ChatGPT, pro realizaci sociotechnických útoků. V souvislosti se zkoumáním aktuálních útoků je nedílnou součástí výzkum a stanovení možností detekce těchto útoků na základě některých pokročilých metod, např. s využitím umělé inteligence (A.I.) a hlubokého učení (DL).

Výzkumným cílem je nalézt, klasifikovat a popsat možné útoky s využitím sociálního inženýrství a navrhnout účinná protiopatření aplikovatelných v reálném provozu.

Literatura:

[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] MONTANĚZ 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