AN EXPERT SYSTEM AS AN AWARENESS TOOL TO PREVENT SOCIAL ENGINEERING ATTACKS IN PUBLIC ORGANIZATIONS

Waldson Rodrigues Cardoso[1], João Marco Silva [2] and
Admilson Ribamar Lima Ribeiro [3]

Federal University of Sergipe, São Cristóvão, Brazil

ABSTRACT

This article highlights the development of an awareness tool in the form of an expert system to prevent social engineering attacks in public organizations. Social engineering attacks have significant consequences for organizations, resulting in security breaches, loss of confidential information, and reputation damage. While protective measures such as awareness training and security policies have been implemented, there is still room for improvement. The tool under development will empower users to identify and avoid psychological manipulation techniques used by attackers, thereby strengthening information security and mitigating associated risks. It addresses key concepts in information security and includes interactive modules based on learning theories, as well as artificial intelligence capabilities to identify vulnerabilities. Once developed and validated, it is expected that this tool will significantly contribute to awareness and protection against social engineering attacks in public organizations, enhancing information security and reducing risks.

KEYWORDS

Social Engineering Attacks, Information Security, Expert System, Awareness, Mitigation.

1. INTRODUCTION

The growing importance of digital information presents opportunities and security risks. The spread of social networking platforms enables attackers to collect employees' data via their online footprints. The information obtained in this manner can then be used to facilitate attacks on an organization. As human decision-making and responsibility play a crucial role in information security, even the strongest technical protective measures are rendered useless if an attacker can successfully influence employees [1].

Social Engineering is a technique used to obtain information through tactics using persuasion, intimidation, coercion, extortion, or blackmail. Social engineers study human behavior, personality traits, and body language to trick or manipulate victims. Social engineering has evolved and adapted into a major cyber-attack technique for gathering information. Today, human error remains the largest reason social engineering attacks are successful [2].

This article presents the development of an awareness tool in the form of an expert system aimed at preventing social engineering attacks in public organizations. The primary objective of the tool is to educate and raise awareness among users, empowering them to identify and avoid the psychological manipulation techniques used by attackers. The proposal aligns with the need to strengthen protection mechanisms against this type of attack, considering the significance of public organizations to society and the increasing sophistication of social engineering attacks.

Dhinaharan Nagamalai (Eds): EMVL, EDUT, SECURA, AIIoT, CSSE -2023
pp. 61-70, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120506

By addressing this challenge, this article contributes to the field of information security by offering an innovative solution that focuses on user awareness as an additional layer of defense. The tool under development goes beyond the dissemination of theoretical knowledge about social engineering and aims to provide users with a practical and interactive experience, strengthening their abilities to identify and respond to manipulation attempts.

Although the tool is still under development, this article provides an overview of its scope, highlighting the planned modules such as the user module based on learning theories, which will enable interaction with information, training, and questions related to social engineering. Additionally, the article mentions the IT manager module, which will be responsible for populating the tool's database, and the risk manager module, which will employ artificial intelligence techniques to infer vulnerabilities based on user interactions.

The structure of this paper is as follows: In Section 2, we explore Related Works, reviewing existing literature and studies in the field. Section 3 provides an overview of the key concepts related to social engineering and expert systems. The Tool Development Proposal is presented in Section 4, detailing the main modules and functionalities of the awareness tool being developed against social engineering attacks. In Section 5, we examine the Expected Benefits and Challenges associated with the adoption of this innovative solution in public organizations. Finally, Section 6 summarizes the Conclusions, offering a comprehensive overview of the findings and insights from this study.

2. RELATED WORKS

This section presents a review of relevant studies related to social engineering in organizations. These studies address the threats and trends of social engineering, mitigation strategies, educational tools, and models to increase awareness and resistance against social engineering attacks.

A study conducted by researchers identified social engineering as one of the most dangerous threats in the current context, due to its potential for stealing confidential information and its negative consequences for organizations [3]. Another research proposed detailed models of social engineering attacks, mapping real-world examples to an attack framework [4]. Additionally, a study introduced a multi-stage analysis approach to social engineering attacks, considering the attacker's accidental factors [5].

Several studies have also explored educational strategies and tools to increase awareness and resistance against social engineering. One work proposed an information technology governance framework applied in a bank, with a focus on phishing attack prevention [6]. Another study developed an immersive virtual reality educational game, called "The Social Engineer," to train players in detecting and resisting social engineering attacks [7].

Furthermore, research has explored the role of employee training and awareness in combating social engineering. One study demonstrated how compliance with information security policies can shape employee behavior and mitigate risks [8]. Another work developed a machine learning-based tool to test employees' resilience against social engineering attacks and promote a culture of information security [9].

In summary, the reviewed studies provide important insights into social engineering in organizations. They address threats, mitigation strategies, educational tools, and models to increase awareness and resistance against social engineering attacks. These findings contribute to

the understanding and development of effective information security practices to protect organizations against psychological manipulation and the disclosure of confidential information. Based on these studies, we have identified some gaps in the literature. However, it is important to note that these gaps present an opportunity for further research and technological advancements in this area. Firstly, there is an opportunity to develop interactive and customized awareness tools tailored specifically for public organizations, considering the unique aspects of this environment. Additionally, exploring advanced attack detection techniques that leverage the potential of artificial intelligence and behavior analysis offers a promising direction for future developments. By addressing these opportunities, we can enhance information security measures against social engineering attacks in public organizations.

To address these gaps, we are developing an awareness tool against social engineering attacks in the form of an expert system specifically targeted at public organizations. The choice to initially focus on public organizations is based on the specific need of this sector to deal with unique challenges and threats they face. Public organizations often handle a high volume of confidential information and are susceptible to attacks that aim to compromise the security and confidentiality of such data. Additionally, laws have been established to establish essential requirements for organizations to provide support and protection for users' personal data, such as the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD) [10]. Therefore, it is essential to develop a tool that takes into account the specificities of this environment, offering tailored solutions and strategies to meet their unique needs. By initially directing our tool towards public organizations, we aim to provide a specialized approach that can effectively strengthen awareness and protection against social engineering attacks in this specific context. However, it is important to emphasize that our tool can be adapted and applied to other organizations as needed.

3. SOCIAL ENGINEERING AND EXPERT SYSTEMS

In this section, we will provide an overview of the key concepts related to social engineering and discuss the importance of awareness and mitigation measures against these attacks. We will discuss the types of social engineering attacks, the mitigating social engineering attacks and expert systems.

3.1. Types of Social Engineering Attacks

Social engineering encompasses a wide variety of techniques used by attackers to psychologically manipulate individuals and gain access to confidential information. The main techniques include phishing, quid pro quo, pretexting, baiting, and tailgating. Each technique is based on either software or human actions and focuses on one or more principles of social engineering. These principles include authority, intimidation, urgency, scarcity, and familiarity. By leveraging psychology and these principles, attackers can convince or deceive victims into clicking on a virus-infected link, inserting an infected USB into a computer, or exploiting common courtesy against them [2].

There are different types of social engineering attacks, which can be categorized into physical, social, technical, and sociotechnical approaches [11].

1) Physical approaches involve physical actions by the attackers, such as dumpster diving, theft, or extortion.
2) Social approaches are based on sociopsychological techniques, such as the use of authority, curiosity, and the creation of relationships with the victims.

3) Technical attacks are primarily conducted through the Internet, taking advantage of people's lack of awareness regarding the disclosure of personal information and the use of weak passwords.
4) Sociotechnical approaches combine different techniques to create powerful attacks.

Social engineering attacks occur across various channels and can be carried out by both humans and software. It is important to note that the boundaries of these attack types are flexible and constantly evolving. Understanding these techniques and their mechanisms is essential for developing effective awareness and prevention strategies.

3.2. Mitigating Social Engineering Attacks

Strategies for dealing with social engineering attacks can be classified into prevention, detection, and mitigation [12]. Under prevention, there are two categories: human user prevention systems and technological prevention systems. Human user prevention systems involve the implementation of policies and processes within the organization, as well as cybersecurity awareness programs and training. Technological prevention systems include website scanning and research, the use of browser extensions like TabShots, and the implementation of a blacklist for malicious traffic.

Detection strategies can be divided into human detection techniques and technological detection techniques. Human detection techniques involve using humans as security sensors, dynamic security covers, and social engineering-centered risk assessment. Technological detection techniques include detecting visually similar phishing web pages using earthmover distance and protection against forgeries.

As for mitigation strategies, they encompass cyber fraud, detection of fake social media accounts, social media awareness, Trojan horse countermeasures, security awareness applied to individuals and organizations, and countermeasures against device-based banking fraud.
Therefore, strategies for dealing with social engineering attacks involve a combination of preventive measures, detection techniques, and mitigation actions.

3.3. Expert Systems

Expert systems were expected to appear in the late 20th century, as private research into the creation and application of artificial intelligence [13].

According to [14], Expert system (ES) is a branch of Artificial Intelligence that makes extensive use of expert knowledge to solve problems at the level of the human expert in a specific domain. For [15], the expert system can be considered as a descriptive programming language because programmers do not need to specify how to perform the specific algorithm. Now, there are various types of expert systems, such as *frameworks* -based expert systems, thought-based expert systems, and rule-based expert systems, and so on.

According to [16], knowledge must be presented in an understandable format to perform any kind of reasoning in the expert system, which is known as knowledge representation. The expert system consists of two components: knowledge base and logical reasoning. The knowledge base is the first component of an expert system and is a collection of information that is in a well-defined representation. The second component of an expert system is the logical reasoner that performs all the necessary thinking on a previously constructed knowledge base. With this logical reasoner we conclude new information from the previously built knowledge base. Several

methods have been adopted in the construction of expert systems in different domains, such as Forward Chaining, Backward Chaining, Fuzzy and the Certainty Method [14].
These methods for constructing expert systems are selected based on the nature of the domain and the characteristics of the specific problem. Each method has its own advantages and limitations, and the appropriate choice depends on the specific application. Moreover, the development of expert systems requires collaboration between domain experts and computer science professionals to ensure an accurate and effective representation of knowledge in the system. These approaches and collaborations contribute to the creation of robust and reliable expert systems in various contexts.

The next section will detail the ongoing development of the tool, describing the key modules and planned functionalities. This innovative approach aims to fill the identified gaps in the literature and make a significant contribution to awareness and protection against social engineering attacks in public organizations.

4. TOOL DEVELOPMENT PROPOSAL

In this section, we will present the proposal for developing an awareness tool in the form of an expert system against social engineering attacks targeted at public organizations. We will describe the main planned modules and functionalities, highlighting their relevance and contribution to strengthening information security in these institutions.

- **User Module:** The user module will be the main interface of the tool, providing an interactive and personalized experience. Based on learning theories, this module will allow users to interact with information, training materials, and questions related to social engineering. Through simulations of real-life situations, users will be challenged to identify manipulation attempts and choose the appropriate response. The user module will also include features to track individual progress and provide feedback to encourage continuous learning.

- **IT Manager Module:** The IT manager module will be responsible for populating the tool's database. This function will enable the registration and monitoring of social engineering incidents within the organization, providing valuable information for analysis and improvement of threat detection. Additionally, the IT manager module will be responsible for updating and adapting the tool's content, ensuring alignment with the latest techniques and trends in social engineering.

- **Risk Manager Module:** The risk manager module will utilize advanced artificial intelligence techniques to provide comprehensive vulnerability analysis. By utilizing the inference method known as Forward Chaining, this module will analyze user interactions and generate reports that allow the manager to accurately diagnose existing vulnerabilities. Applying this inference method, the expert system will identify patterns and root causes of the problems, enabling an effective response to the identified vulnerabilities. Furthermore, the Risk Manager Module will also employ machine learning techniques to complement its capabilities. These techniques will allow the system to train machine learning models based on labeled historical data and identify subtle patterns and unusual behaviors in user interactions. This combination of inference method and machine learning enhances the accuracy of the analysis and the system's responsiveness, enabling effective mitigation of the identified problems. With this combination of techniques, the Risk Manager Module will offer a detailed insight into existing vulnerabilities, providing the manager with the necessary information to take proactive measures and redirect the content presented by the tool.

By integrating these three modules into a comprehensive platform, the tool under development, in the form of an expert system, will provide a holistic approach to awareness and protection against social engineering attacks in public organizations. Personalized interaction will allow users to receive training and relevant information according to their needs and levels of knowledge. Tracking individual progress will enable the evaluation of the effectiveness of awareness strategies and identify areas that require further attention.

The analysis of user behavior, combined with advanced artificial intelligence techniques such as machine learning, will offer a powerful approach to detecting social engineering attacks and actions. By utilizing labeled historical data, the system will be able to train models to classify user interactions into different categories, identifying subtle patterns and unusual behaviors that may indicate malicious activities. This combination of techniques enables comprehensive detection and faster response, enabling early identification of potential threats and social engineering actions, thereby reducing the impact of these attacks.

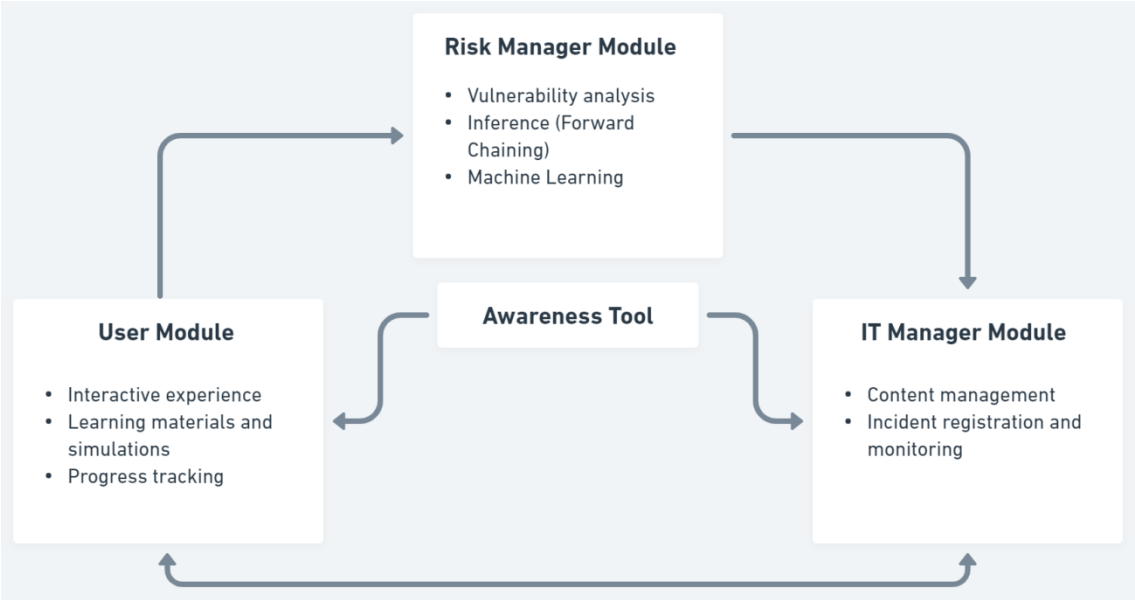

Figure 1. Illustrates a developing awareness tool against social engineering attacks in public organizations, highlighting specific modules and their interaction to enhance information security and mitigate risks.

To visualize the interaction between the modules and how the tool will address awareness and protection against social engineering attacks in public organizations, refer to (Figure 1)
.
The development of an awareness tool in the form of an expert system aims to provide a comprehensive approach to awareness and protection against social engineering attacks in public organizations. The implementation will utilize the Laravel Framework, a popular and robust PHP-based web application framework known for its elegant syntax, ease of use, and extensive features. Leveraging the power of Laravel, we can efficiently design and build the user module, IT manager module, and risk manager module with seamless integration and a user-friendly interface.

For database management, we will employ PostgreSQL, a powerful open-source relational database management system known for its scalability, performance, and support for advanced data types. As the expert system will handle sensitive information and user interactions, ensuring data security and efficient data management are crucial. PostgreSQL provides robust features for

handling complex data structures and querying, making it a suitable choice for storing and managing the diverse data involved in the expert system.

To enhance the ability to detect social engineering attacks, our expert system utilizes the Forward Chaining method, an inference technique that allows real-time analysis of user interactions to identify potential threats. By implementing Forward Chaining, the system performs progressive reasoning, applying rules and inferences iteratively based on the data received from user interactions.

When a user interacts with the expert system, Forward Chaining analyzes their actions and checks if they correspond to any previously identified suspicious patterns or behaviors. If a sequence of interactions matches a potential social engineering attack scenario, the system can take preventive measures or alert the user about the potential threat. In this way, Forward Chaining enables faster and more proactive detection of psychological manipulation attempts and malicious attacks.

Regarding the machine learning model, we will implement a supervised learning approach for social engineering attack detection. First, we will preprocess the labeled historical data, which will serve as the training dataset for the machine learning model. The data preprocessing phase involves data cleaning, feature extraction, and data transformation to ensure that the input data is in a suitable format for the machine learning algorithm.

Next, we will employ a classification algorithm, such as Support Vector Machines (SVM), Random Forest, or Neural Networks, to train the machine learning model. The selected algorithm will learn from the labeled historical data, identifying patterns and relationships between user interactions and social engineering attacks.

Once the machine learning model is trained, we will integrate it into the risk manager module. As users interact with the expert system, the risk manager module will continuously analyze their interactions and feed the data into the machine learning model for classification. The model will then classify the interactions into different categories, such as normal interactions or potential social engineering attacks, based on the learned patterns.

The risk manager module will generate detailed reports based on the machine learning model's output. These reports will provide insights into existing vulnerabilities, user behavior patterns, and potential threats, enabling the IT manager to take proactive measures and enhance the expert system's content accordingly.

By leveraging the power of machine learning, the expert system will continuously improve its ability to detect social engineering attacks and provide faster responses to potential threats, ultimately enhancing information security measures in public organizations.
By incorporating these technologies and methodologies into the development of the expert system, we aim to create a sophisticated and effective tool that empowers public organizations in their fight against social engineering attacks and strengthens overall information security practices.

The next section of the article will provide information about the expected benefits and challenges for public organizations that adopt this innovative solution.

5. EXPECTED BENEFITS AND CHALLENGES

In this section, we will discuss the expected benefits of implementing the social engineering awareness tool, as well as the challenges that may arise during the development and deployment process.

The implementation of the social engineering awareness tool is expected to bring several benefits to public organizations in combating social engineering attacks. Firstly, the tool will provide users with essential knowledge about social engineering and psychological manipulation techniques, empowering them to recognize and avoid such attacks. By raising awareness and creating a security culture, users will become less susceptible to manipulations. Secondly, the tool will include a risk manager module that utilizes advanced artificial intelligence techniques to identify potential vulnerabilities based on user interactions. This proactive approach will allow organizations to adopt preventive measures before social engineering incidents occur, thereby strengthening their information security. Lastly, the tool will have features for feedback and tracking individual users' progress. This will enable organizations to identify areas for improvement and adapt the tool's content based on users' needs, promoting a continuous process of awareness and prevention enhancement against social engineering attacks.

While the implementation of the tool brings significant benefits, there are also challenges to consider during the development and deployment process. One challenge is ensuring user engagement and active participation in the tool. Motivation and incentive strategies will need to be developed to encourage users to regularly use the tool and engage in the proposed activities. Another challenge is the continuous maintenance and updates of the tool. Information security is a rapidly evolving field, and it is crucial to keep the tool relevant and effective in combating emerging social engineering threats. Additionally, integrating the tool with existing systems and processes in public organizations may pose a challenge. Compatibility with existing IT infrastructures needs to be ensured, while also considering privacy and security aspects in handling the collected data.

By addressing these challenges appropriately, it is possible to maximize the benefits of the tool and ensure its effectiveness in raising awareness and preventing social engineering attacks.

6. CONCLUSIONS

Training employees on various types of social engineering attacks can be one of the most effective preventive measures to protect against falling victim to such attempts. Additionally, raising awareness about potential phishing scams circulating within an organization is crucial in bolstering defense against social engineering attacks.

Awareness and prevention against social engineering attacks are essential elements in protecting information security in public organizations. The highlighted tool in this article has the potential to significantly contribute to this objective, empowering users to recognize and avoid psychological manipulation techniques.

However, it is important to highlight that the development and implementation of this tool will face challenges and require ongoing efforts. Collaboration between information security professionals, social engineering experts, and software developers will be crucial for the success of the project.

Furthermore, it is important to consider the need for a multidisciplinary approach, involving technical, behavioral, and educational aspects. Awareness against social engineering attacks should be an ongoing effort, embedded in the daily practices of public organizations.

In conclusion, the tool under development has the potential to strengthen information security in public organizations, empowering users to protect themselves against social engineering attacks. With proper implementation and the commitment of stakeholders, it is possible to mitigate risks and promote a safer and more trustworthy environment for information sharing.

ACKNOWLEDGEMENTS

We, the authors of this article, would like to express our gratitude to our supervisor for the assistance provided in completing this research. We also want to thank our university, the Federal University of Sergipe, Brazil, for their support, as well as CAPES through the Graduate Program Development Program (PDPG) – Strategic Partnerships in States III. Your support has been fundamental to the accomplishment of this work.

REFERENCES

[1] T. Grassegger and D. Nedbal, "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering," in Procedia Computer Science, vol. 181, pp. 59-66, 2021. doi: 10.1016/j.procs.2021.01.103.

[2] A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang, and H. N. Thakur, "Social engineering incidents and preventions," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023, pp. 0494-0498.

[3] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," in *2015 International Conference on Cyberspace (CYBER-Abuja)*, 2015, pp. 91-100.

[4] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," in *2015 International Conference on Cyberspace (CYBER-Abuja)*, 2015, pp. 91-100.

[5] A. Khlobystova and M. Abramov, "Time-based model of the success of a malefactor's multistep social engineering attack on a user," in *SPRINGER International Conference on Intelligent Information Technologies for Industry*, [S.l.], 2021, pp. 216-223.

[6] R. A. Hammour et al., "The status of information security systems in banking sector from social engineering perspective," in Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems (DATA '19), New York, NY, USA, 2019, ISBN 9781450372848, pp. N/A. doi: 10.1145/3368691.3368705.

[7] P. Jansen and F. Fischbach, "The social engineer: An immersive virtual reality educational game to raise social engineering awareness," in Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play (CHIPLAY '20), New York, NY, USA, Association for Computing Machinery, 2020, pp. 59-63, ISBN 9781450375870, doi: 10.1145/3383668.3419917.

[8] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," in Computers & Security, vol. 56, pp. 70-82, 2016, ISSN 0167-4048, doi: 10.1016/j.cose.2015.09.006.

[9] L. Astakhova and I. Medvedev, "Scanning the resilience of an organization employees to social engineering attacks using machine learning technologies," in 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), [S.l.], 2020, pp. 606-610, doi: 10.1109/USBEREIT51578.2020.9256762.

[10] E. T. V. de Castro, G. R. S. Silva, and E. D. Canedo, "Ensuring Privacy in the Application of the Brazilian General Data Protection Law (LGPD)," in Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, pp. 1228-1235, Virtual Event, 2022.

[11] K. Krombholz et al., "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113-122, 2015. ISSN 2214-2126. Special Issue on Security of Information and Networks.

[12] M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, and N. Kaabouch, "Social Engineering Attacks: A Reconnaissance Synthesis Analysis," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2020, pp. 0843-0848, doi: 10.1109/UEMCON51285.2020.9298100.
[13] E. S. Mandrakov, V. A. Vasiliev, and D. A. Dudina, "Application of expert systems in quality management," in 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies, [S.l.], 2021, pp. 516-518.
[14] S. W. Sihwi, F. Andriyanto, and R. Anggrainingsih, "An expert system for risk assessment of information system security based on ISO 27002," in *2016 IEEE International Conference on Knowledge Engineering and Applications (ICKEA)*, 2016, pp. 56-61.
[15] J. Yu, P. Tian, H. Feng, and Y. Xiao, "Research and design of subway based intrusion detection expert system," in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2018, pp. 152-156.
[16] C. Rani and S. Goel, "CSAAES: An expert system for cyber security attack awareness," in *International Conference on Computing, Communication Automation*, 2015, pp. 242-245.

AUTHORS

Waldson Rodrigues Cardoso, MSc Student.
2016: Degree in Information Systems, UFS, Brazil.
2019: Specialization in Team Management and Project Feasibility, FUNIP, Brazil

João Marco Silva, I am an assistant researcher at INESC TEC.
2008: Degree in Computing Science, UFS, Brazil.
2011: Master in Engineering and Communication Services, UM, Portugal.
2016: PhD in Informatics, UM, Portugal.

Admilson de Ribamar Lima Ribeiro,
Teacher of Computing Science, Federal University of Sergipe.
1981: Degree in Electrical Engineering, UFPA, Brazil.
2001: Master in Computer Science, UFPE, Brazil.
2007: PhD in Electrical Engineering, UFPA, Brazil.