Dmytro Zatonatskiy
National Institute for Strategic Studies,
Kyiv, Ukraine
dzatonat@gmail.com

INSIDER THREAT MANAGEMENT DURING COVID-19 PANDEMIC

JEL Classification: M12, M54

ORCID ID: 0000-0002-4828-9144

Abstract

It became apparent that the process of the digitalization, COVID-19 pandemic, and the transition to a remote format for most employees caused a new wave of updated research in the field of personnel and information security, mainly regarding insider threat management to minimize the risk of losing important information due to accidental or intentional actions of employees. We propose to utilize the approach featuring the synergistic system of indicators that can be used individually or in combination, depending on the individual needs of the enterprise. The result of the study is the development of an expert system using the corporate network based on the emotional state of employees and the manifestation of behavior atypical for the employee of the company, which allows to identify employees whose behavior shows an increased risk of damage or loss of confidential information.

Keywords: personnel security, insider threat management, expert system, Data science, personnel, information leaks.

Introduction

Nowadays, it is important to realize that technologies and tools to prevent risks and threats of leakage of confidential information must be systematic and go beyond formal control rules. A person has always been and remains the carrier and source of strategically important information, no matter how perfect the forms of accumulation and channels of information transmission are.

The aim of the study is to develop a system of models of insider threat management of enterprises as a part of its economic security based on the advanced tools of Data

science.

The use of advanced insider threats management practices will reduce the risk of losses caused by the breaches of the economic security system due to leaks of confidential information, and will correct the behavior of employees before the negative factor becomes critical. It is established that in existing conditions an important area of the insider threat management is the development of an effective control system for the remote operations of the enterprise.

Research Results

The increased risk of insider threats is due to the increasing number of points of access to confidential information and the inability to fully control the devices from which the work is performed, because they are not connected to the company's internal or local network. At the same time, experts recommend providing remote employees with company devices for work, raising awareness of the personnel about possible threats, it is also important to create an algorithm in case of cyber-attacks and to develop protocols for responding to insider attacks. To protect against the above mentioned threats, the company can create a secure remote network, which involves the development of security infrastructure, such as individual security protocols, meaning VPNs or remote workstations. It became very popular for the employee to connect through their equipment to a remote server, which can be located in any country, and to work only at the desktop, with the data that is on this server, he cannot copy data to his device.

To create its own customized concept, a company must first determine the level of its vulnerability to internal threats. In case of the company having low vulnerability to internal threats, standard frameworks can be used, such as training staff in basic safe online behavior and using standard software. If the company has a medium level of vulnerability, it is advisable to use international standards of personnel security, as well as to monitor the activities of the employees in the network. To further increase the level of insider threats security, various anomalies should be identified when analyzing the behavior of users in the corporate network (including the use of computers, the Internet, e-mail). Thus, the main idea of this approach is to identify potential employees who behave in a manner atypical for the company using the corporate network.

It was found that at the present stage of development of the models and approaches to the insider threats management there are two main approaches: psychosocial

models and monitoring of computer activity of the employee. The psychosocial approach can be considered prognostic, because with its help the company tries to determine whether the employee poses a potential threat to economic and personnel security to predict his future actions. Instead, activity monitoring involves the use of technical strategies that, based on tracking the actions of an employee in the network, allow to establish his involvement in an insider attack.

One of the commonly-used models under this approach is the most well-known model OCEAN. It makes it possible to establish a link between threats and counterproductive behavior of workers at the workplace. This model describes the following 5 personal factors such as emotional stability, extraversion, openness to experience, cooperation, honesty. These factors, if properly assessed in a timely manner, can alert an organization to the development of personnel crime among employees.

Discussion and Conclusions

The approach based on identifying employees who show an increased risk of insider threat has two advantages: first, it prevents unnecessary costs for the employer due to the loss of confidential information and helps the employee before the negative factor becomes critical. Thus, an expert system based on a psychosocial model will benefit both employees and employers if this model is adopted by the company as one of the tools to ensure personnel security and is included as an instrument for staff evaluation.

References

1. Zatonatskiy D. Innovation methods and models of personnel security management: opportunities and imperatives of use at Ukrainian enterprises Маркетинг і менеджмент інновацій. – 2019. - №1. – С. 294-301.
2. Zatonatskiy D., Dluhopolska T., Rozhko O., Tkachenko N., Stechyshyn T., Metlushko O. Modern information technologies in HRM: concept of personnel security // 2019 IEEE International Conference on Advanced Trends in Information Theory, Kyiv,18-20 December 2019, p. 313-316.
3. Zatonatskiy, D., Marhasova, V., & Korogod, N. (2021). Insider threat management as an element of the corporate economic security. Financial and Credit Activity: Problems of Theory and Practice, 1(36), 149–158. https://doi.org/10.18371/fcaptp.v1i36.227690.