Proceedings of International Conference on Educational Discoveries and Humanities
Hosted online from Plano, Texas, USA.
Date: 1st January, 2024
ISSN: 2835-3196 **Website:** econferenceseries.com

METHODS OF TAKING MEASURES FOR IDENTIFIED ILLEGAL ACTIVITIES

Anvarjon Abdujabborovich Maxkamov
International Islamic Academy of Uzbekistan, Senior teacher of the "Department of Modern ICT" mahkamovanvar2020@gmail.com 11, A.Kadiri, Tashkent, 100011, Uzbekistan.

Alimjon Irgashevich Dadamuhamedov
International Islamic Academy of Uzbekistan, Senior teacher of the "Department of Modern ICT" a.dadamuxamedov@iiau.uz 11, A.Kadiri, Tashkent, 100011, Uzbekistan.

Abstract

In today's digital era, methods of taking measures against detected illegal activities are one of the most important problems. Taking action against detected illegal activities is one way to ensure network security. In this article, the methods of taking measures against illegal activities detected in the network are considered.

Keywords: digital technology, network, permissions, software, data, security, threat.

When illegal behavior is detected on the network, it is important to take appropriate measures to mitigate the threats and protect the network and its users. Let's take a look at some common ways to take action against detected illegal activity.

Incident Response: An incident response plan should be implemented to determine the actions that need to be taken when illegal activities are detected. This plan should outline the roles and responsibilities of the incident response team, the communication process, and the actions to be taken to contain and investigate the incident.

Isolation and Containment: It is necessary to isolate affected systems or devices from the network to prevent further damage and limit the spread of illegal activity. This includes disconnecting compromised devices, quarantining infected files or users, or isolating network segments.

Remediation and Cleanup: Actions will be taken to remove or neutralize illegal activity from the network. This includes removing malware or unauthorized access points, patching vulnerabilities, recovering compromised credentials, or restoring affected systems from a clean backup.

Strengthening security controls: Security controls and measures need to be strengthened to prevent similar incidents in the future. This includes updating and patching software, implementing stronger access controls, improving network monitoring and logging, and providing security training for users.

Cooperation and reporting: Information about detected illegal activity will need to be reported to appropriate stakeholders, such as law enforcement agencies, security vendors, or other affected organizations. Cooperation and reporting can help investigate the incident, track down the perpetrators, and prevent future attacks.

Continuous monitoring and improvement: It is necessary to establish continuous monitoring of the network to detect and respond to any illegal activities. Investigate past incidents to regularly review and update security measures, conduct security audits, and improve the overall security posture of your network.

It is important to adapt the measures taken depending on the specific nature and severity of the detected illegal actions. Organizations should also comply with legal and regulatory requirements and consult with cybersecurity experts or incident response experts as needed.

References:

1. Mahkamov, A. A., Jumayev, T. S., Tuhtanazarov, D. S., & Dadamuxamedov, A. I. (2024). Using AdaBoost to improve the performance of simple classifiers. In Artificial Intelligence, Blockchain, Computing and Security Volume 2 (pp. 755-760). CRC Press.
2. Papadopoulos, S., Kompatsiaris, Y., & Vakali, A. (2018). Network analysis and mining for social media. Synthesis Lectures on Data Mining and Knowledge Discovery.
3. Zhang, D., Liu, Y., & Wu, Y. (2020). Network traffic anomaly detection based on gradient boosting decision tree algorithm. Computer Communications.