GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 6 June (2024)

WAYS TO FIGHT AGAINST COMPUTER CRIME

Haydarov Elshod Dilshod ugli,
Doctor of Philosophy in Technical Sciences (PhD) Tashkent
University of Information Technologies named after Muhammad al-Khwarazmi

ABSTRACT

Combating cybercrime requires a comprehensive approach. Given that technical measures alone cannot prevent crime, law enforcement agencies need to improve the effective investigation and punishment of cybercrime. In this thesis, comprehensive approaches to combating cybercrime are presented.

Keywords: cybercrime, security culture, digital asset management, technical solution, legal and legal framework, pentesting.

INTRODUCTION

It is necessary to solve legal problems arising from crimes committed on the Internet at the international level. Cybercriminals are prepared to infiltrate the Internet network of a strongly protected or weakly protected country or company. Therefore, "International cooperation" is necessary to fight against cybercrimes, because cybercriminals are breaking the Internet of all protected countries. Cyber crimes are mainly committed in developing or developed countries. This is because banks, companies, large manufacturing organizations, and trading of money or securities in the markets are popular and abundant in these countries. The need of the hour is to unite to fight against them. Cybercriminals attack some large corporations or companies and threaten them to reduce their customers, and they use this to express their goals. And companies have no choice but to agree to this, because they fear that their products will not sell or users will decrease, and they will hide the situation from the public. This will be the first defeat in the fight against cybercriminals. Cybercriminals are inspired by this and prepare to attack other companies. Some cybercriminals make this a hobby and prove themselves to be capable of many things by hacking into protected networks or to test the strength of their protection. But some individuals are using them for their own purposes after gaining their trust. After achieving his goals, he becomes a full-fledged subject of cybercrime, wanting to achieve even greater things. In order to stop them, it is necessary to form a strong cyber security system and cyber security personnel. Nowadays, the number of cyber attacks is increasing every second. This indicates millions of attacks. The development of laws against cybercrime and the formation of a legal framework for cybercrime, the increase and application of legal measures against cyber security are an integral part of the cyber security strategy. Preventing computer crime requires a systematic, comprehensive approach. Every organization and user must regularly update their security systems and protection methods, as well as adapt to new threats and technological developments.

Deeper approaches are needed to combat computer crime. The following methods are important in the security strategy of every organization and we will analyze them in more detail:

Develop a safety culture within the organization

• Regular employee training: Regularly educate employees about new security threats and how to counter them.

• Simulated Attacks: Testing employees on how to counter phishing and other fraud schemes. This allows you to see how they act in real situations and provide additional training if necessary.

Digital asset management

• Data protection policy: Limiting access to and making copies of important data. Back up data regularly and provide access to it only to appropriately authorized personnel.

• Separate storage of confidential information: Keep important information on separate, well-protected servers.

Expansion of technical solutions

• **IDS/IPS systems:** monitor networks and identify potential threats by installing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

• Virtual Private Networks (VPN): Using VPN to secure remote employees. This ensures secure data transfer.

Legal and legal grounds

• Document security policies: Clearly document all security procedures within the organization. These documents help employees understand their security responsibilities.

• Establishing security requirements in contracts: Establishing security standards in contracts concluded by the organization with external service providers.

Regular inspection of systems

• Security Audits: Conduct regular security audits of systems to identify and eliminate system vulnerabilities.

• Pentesting: Testing the robustness of systems through attempts to break their security by specialized experts or external auditing companies.

Such complex approaches allow effective fight against computer crime and play an important role in protecting organizations from various risks.

There are additional strategies and techniques for organizations and users to combat computer crime. We will analyze them below:

Digital signature and data identification technologies

• Digital signatures: Using digital signatures to ensure the authenticity and integrity of data and software. This method helps to detect illegal changes to documents and programs.

• DLP (Data Loss Prevention) systems: Implementation of DLP systems to combat data loss. These systems protect data inside or outside the organization by detecting and blocking improper data exchange.

Strengthening cyber security

• Collaboration with cybersecurity experts: Stay in touch with industry experts to stay informed about cybersecurity news and threats.

• CyberSecurity Tools: Organizations must use the latest cyber security tools and technologies. These tools include cybersecurity platforms, intrusion detection systems, and automated security solutions.

Protection of personal data

• Development of a privacy policy: The rules of how to collect, store and use personal data of users should be clearly defined.

• User Control: Give users control over their data, such as the right to delete or edit their data.

Contingency plans

• Develop a contingency plan: Organizations should have a contingency plan to counter various cyber attacks. This plan includes how the organization will respond, how to mitigate adverse effects, and how to quickly restore operations.

• Continuous assessment and updating: The emergency plan and other safety protocols should be continuously evaluated and updated. This allows us to adapt to the changing threat landscape and the development of technologies.

These approaches help organizations effectively combat cybercrime and protect their networks and data. Cybersecurity is not only a technical issue, but also a management, employee training and organizational policy issue.

REFERENCES

1. А.Н.Попов Преступления в сфере компьютерной информации. Учебное пособие, Санкт-Петербург 2018.
2. Е. В. Вострецова Основы информационной безопасности. Екатеринбург Издательство Уральского университета 2019.
3. Жужгина А. А. Международное сотрудничество в сфере уголовного процесса: проблемы экстрадиции киберпреступников // Молодой ученый Международный научный журнал. 2020. № 2(311). С. 249–323.