ETHIOPIAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 11, Issue 06, June-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

THE ROLE OF NEW TECHNOLOGIES IN PROVIDING INFORMATION SECURITY IN CAPARATIVE NETWORKS

Akhmatova Sitorabonu
Teacher at University of Information
Technology and Management in Karshi, Uzbekistan
Pardaeva Gulmira
Teacher at Karshi branch of Tashkent University of
Information Technologies named after Muhammad al-Khwarizmi

Annotation: In this article, the introduction of modern technologies to ensure information security in corporate networks, as well as the goals and objectives of the technologies used and the introduction of additional innovative changes to improve their performance, are highlighted on a scientific basis.

Keywords: Information security, security technologies, corporate networks, authentication, big data (Big Data), real-time monitoring, transaction confirmation, quantum encryption, cloud security technologies

Ensuring information security in corporate networks is one of the urgent issues, and the role of new technologies in ensuring information security in corporate networks is of great importance. security has been significantly improved with the introduction of modern technologies. Below you can get acquainted with the latest and most effective technologies used in this field:

New modern security technologies such as AI, Trust Architecture, Blockchain, SOAR platforms, Transaction Confirmation, cloud security technologies, with the ability to identify threats and respond to them in real time. These technologies analyze user behavior, detect unusual activity, and automatically take action.

Blockchain Technology: Using blockchain technology to ensure data integrity and transparency, data is encrypted and stored in a decentralized network, which ensures that data is not altered and protected from fraud.

Confirmation of transactions: Increases the security of financial and trading transactions. Every login is constantly required to be authenticated, even on an internal network. This approach increases security within the network.

Greater security control: Access rights are strictly controlled and the principle of least rights is implemented, making it difficult for attackers to gain access to the network.

Cloud Security Technologies: Monitor and manage the security of cloud infrastructure through Cloud Service Security Platforms (CSPM).

Cloud security tools include encryption, authentication, and access control services to protect these applications and data.

Big Data and Analytics Threat Analysis: Early detection and prevention of cyber threats by analyzing large volumes of logs and transactions. Real-time monitoring provides real-time monitoring of the cyber security situation and rapid response to problems with the help of big data analytics.

Rescue and Responder Automation (SOAR):

Automated Security Operations These SOAR platforms provide automated response to cyber attacks and security incident management. Integrated Systems These SOAR systems respond quickly and efficiently to security incidents by integrating various security tools and platforms.

Quantum Encryption: Defense Against Quantum Computers: Quantum encryption techniques are used to protect data from being tampered with by quantum computers. It is an important technology for future cyber security.

Persistent authentication: The Zero Trust model requires constant authentication of users, devices, and applications, even across internal networks. This approach increases security.

Artificial intelligence and machine learning, blockchain, zero-trust architecture, cloud security, big data analytics, SOAR and quantum encryption technologies can improve the security of corporate networks and effectively combat cyber threats. Ensuring information security in corporate networks is one of the most important issues of the present time. For businesses, information is a commodity that needs to be efficient, secure, and aggressively protected. This problem has become a common target for hackers and hackers. Therefore, ensuring information security in corporate networks, initially, includes cyber-attacks, information leakage, violation of data discipline, ensuring user identification and protection of confidential information.

In order to solve this problem, several measures should be implemented, the production of specialist personnel in the field of cyber-security, a set of specialists for the protection of corporate networks, and the prevention of hacking are necessary. This forces them to update themselves and implement new security practices. Protecting confidential information: In corporate networks, it is necessary to protect information in processes such as ensuring the identification of users, protecting confidential information, increasing the level of confidentiality and encoding confidential information. Use network scanners and monitoring tools: Network attacks can be protected by installing network security points and monitoring systems.

Security protocols must be used for data encryption, data transmission, and data reception during data transmission protection.

Set up multi-factor authentication: Second-level authentication systems, such as sending SMS codes or setting up multi-factor authentication, can help improve user identification.

Regular network audits: Hacking tools and hardening testing help monitor corporate networks for security breaches.

Educate users about security: Users should be educated about privacy and security principles.

When it comes to information security in corporate networks, it's important to make serious decisions, establish privacy policies that are appropriate for each company, and implement attack protection processes.

User security is a key part of ensuring privacy in corporate networks. Users can be a network's hardest hit, so it's important to educate them about security and provide them with the tools they need. The following steps are important in setting up user security:

Structure of the security policy It is very important to structure the security policy of the company. This policy explains to users what actions they should take, such as not downloading malicious files, not being aware of unknown sources, and being aware of security risks. Educate users: Explain the company's security policy to users. This includes teaching important practices such as keeping information confidential, using strong passwords, being careful when sending information, and so on. Authentication protocols: It is important to establish strong authentication protocols to ensure user authentication. Using multi-factor authentication, biometrics, or other authentication methods can help keep users more secure.

Data Protection: Users should be taught how to protect data. This includes training in privacy, using encrypted files, and implementing appropriate privacy practices.

Security Monitoring: It is important to use monitoring tools to monitor user activity and focus on privacy. This allows monitoring of user activity and data access. Protection against corruptions: Users should learn to pay attention to security risks. This includes intercepting data, carefully changing data, and paying attention to your security setup, not just before an attack, but after it happens. User security organization is a large part of providing robust and effective security for enterprise networks. This step ensures that how users focus on security and protect their personal information.

Summary

Security is important not only in protecting systems, but also in improving the security of people. Users and staff should be trained in security. In addition, it requires a multi-factorial approach to privacy to protect personal data, using the tools provided for automatic distribution management, network monitoring and privacy.

References:

1. W. Caijun, J. Xi and Z. Zhenzhou, "Analysis of Systematic Reform of Future Teaching in the Age of Artificial Intelligence," 2021 2nd International Conference on Artificial Intelligence and Education (ICAIE), Dali, China, 2021, pp. 704-707.
2. Z.R.Rakhmonov, G.A.Pardaeva. Steps Of Organizing The Methodology Of Improvement Of Methods Of Distance Learning Of Students // 2021 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent, Uzbekistan. (SCOPUS). 3-5 Nov. 2021.
3. X. Wei and H. Jia, "A Review of the Application of Artificial Intelligence in the Virtual Learning Environment," 2021 Tenth International Conference of Educational Innovation through Technology (EITT), Chongqing, China, 2021, pp. 79-82, doi: 10.1109/EITT53287.2021.00024.
4. Z.R.Rakhmonov, G.A.Pardaeva. Mobile application development education methodology with integrated distance learning environment // Central Asian Journal of Education and Computer Sciences VOLUME 1, ISSUE 2, APRIL 2022 (CAJECS), ISSN: 2181-3213