Protectıon Of Enterprıse Informatıon

Yagub Sardarov, Nadir Rahimov

Abstract

As the evaluation of information assets increases, the need to protect them becomes even more crucial. Failure to safeguard the enterprise's information resources or to implement adequate security measures can result in serious consequences. The focus is on the risks that can obstruct the primary information resources of the enterprise in its operation. At the same time, the discussion alsoaddresses the more effective and cost-efficient means of mitigating the identified risks. In our modern digital era, protecting information resources is crucial for every company. This necessitates the implementation of a strong security policy and measures to protect sensitive information from cyber threats such as hacking, malware, and phishing attacks. To effectively protect information resources, companies should regularly perform risk assessments, develop comprehensive security policies and procedures, and utilize various security technologies such as firewalls, intrusion detection systems, and encryption tools. Furthermore, companies should ensure that their employees receive cybersecurity training and understand the risks associated with managing information. By implementing appropriate security policies, procedures, and technologies, companies can protect the confidentiality, integrity, and availability of their information resources while also maintaining their reputation and compliance with regulatory requirements.

After analyzing the main security measures, encryption algorithms are identified, and then the security program of the enterprise is elaborated.

Key words: Security measures, encryption algorithms, protection, security policies.

Protection of information resources within an organization is of critical importance for ensuring business continuity. These resources can include financial data, customer records, intellectual property, and employee information, as well as hardware and software components. To safeguard these resources, companies must implement a range of physical and digital security measures to mitigate potential risks.

Physical security measures encompass control of access to buildings, employee workstations, and server rooms, while digital security involves protecting computer systems and networks from harmful attacks and unauthorized access [1, 2]. Each organization uses various methods to protect its information resources. The main protection methods may include encryption, security programs, access control, data backups, security policies, employee training, monitoring, and auditing.

A comprehensive security policy outlines the security measures that must be taken to protect an organization's information resources. It covers topics such as physical and digital security, data classification, access control, incident response, and disaster recovery. Employee training programs ensure that employees are aware of the risks associated with information security and understand their role in protecting the organization's resources. Monitoring and auditing can help identify security breaches and potential vulnerabilities, allowing organizations to take appropriate measures to address them.

In conclusion, the protection of information resources is a critical aspect of organizational security, and effective security measures must be implemented to mitigate potential risks. The use of encryption, security programs, access control, data backups, security policies, employee training, monitoring, and auditing can help organizations safeguard their information resources against physical and digital threats.

Encryption. Encryption is a widely used technology in the field of information security that allows for sensitive information to be encrypted, thereby preventing unauthorized access. Encryption employs mathematical algorithms to render plaintext information "meaningless". These algorithms use keys to encrypt information and allow only authorized parties with the correct key to decrypt and read the information [3, 4]. The two most commonly used types of encryption are symmetric (Figure 1) and asymmetric (Figure 2). Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption employs two keys, one for encryption and another for decryption.

Symmetric encryption is a commonly used technique in information security. It involves using the same key for both encryption and decryption of sensitive information. Some well-known symmetric encryption algorithms include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) [4].
Asymmetric encryption is a cryptographic technique that uses different keys for encryption and decryption. In this method, a public key, also known as an encryption key, is used to encrypt the message, while a private key, also known as a decryption key, is used to decrypt it. Some well-known asymmetric encryption algorithms used for encryption and decryption include RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm), and ECC (Elliptic Curve Cryptography) [4].

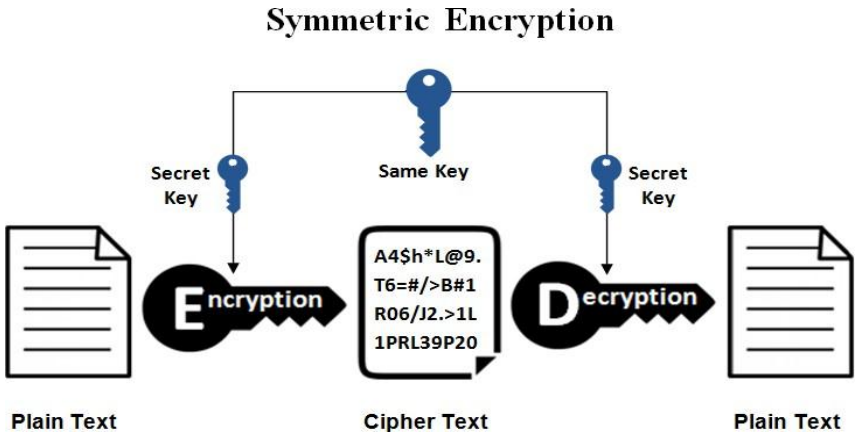

Figure 1. Symmetric Encryption

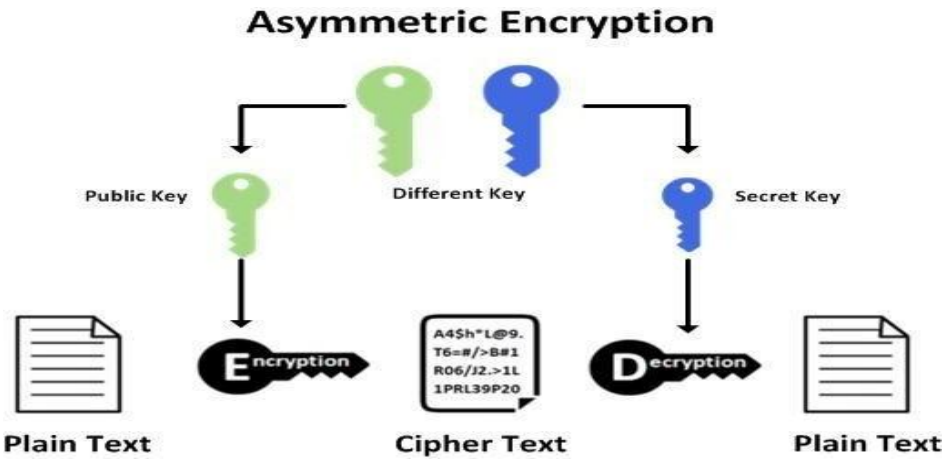

Figure 2. Asymmetric encryption

Hybrid encryption is a combination of symmetric and asymmetric encryption methods. This method provides a more secure encryption technique and can use both symmetric and asymmetric encryption methods.
Block cipher encryption is a cryptographic method that divides data into blocks and encrypts each block separately (Figure 3). This provides a more secure encryption but may result in longer processing times [4].

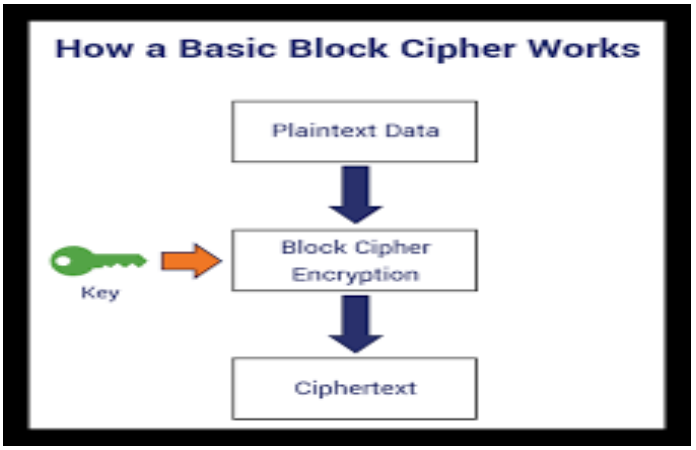

Figure 3. Block cipher encryption

Security Program. The security program is available for both individual users and corporate environments, and typically performs the following functions:
1. Virus and malware scanning - it scans the system for malicious software and detects them.
2. Firewall - it blocks malicious or unwanted traffic from the internet connection.
3. Authentication - it authenticates users and prevents unauthorized access.
4. Encryption - it ensures the security of sensitive information by encrypting it.
5. Update check - it ensures the security program is regularly updated to enhance defense against new threats.
The security program is designed to combat hackers, viruses, worms, spyware, and other threats. When selecting an appropriate security program for any device, it is important to choose the relevant program software based on the type of threats and the needs of the device [5].
The main objective of implementing access control is to ensure that information can only be accessed by authorized individuals. Access control is a security measure aimed at managing and limiting users who have access to a system or resource. Access control encompasses authorization, authentication, and permission steps. Authorization is a process that determines which resources a user can access. This process is governed by a set of policies that determine the user's roles and responsibilities. Authorization is often based on factors such as the user's identity or group membership. Authentication is a process that confirms the credentials provided by the user are valid for access. Authentication may utilize methods such as passwords, pins, biometric authentication, smart cards, or any other authentication method [5, 6].
The operation of creating backup copies of information refers to copying the data to another location. These copies can be used in case of data loss. The backup copies of data can be created manually or automatically. The automatic backup process ensures that the data is backed up regularly without requiring manual intervention. Cloud services such as Google Drive, Dropbox, onedrive allow users to create backup copies of their data. There are also paid backup tools available such as Carbonite, Acronis True Image, and others [5].
The security policy is a guiding document created to protect an organization from security risks. This policy constitutes a fundamental document that specifies the security strategy and approach of the organization. The security policy is intended to assist the organization in mitigating risks to its business continuity, reputation, and customer security. As a result, it is imperative for organizations to allocate time and resources to create and implement a security policy. [3, 7].
Monitoring and inspection are important processes for providing information on the implementation and

effectiveness of an organization's information security policy. Monitoring is used to control the effectiveness of the organization's information security efforts. Audit, on the other hand, is an examination conducted to determine the compliance of the organization with its information security policies. The inspection process encompasses the evaluation of the consistency, correctness, and adequacy of the security policies implemented in the organization [3, 8].

In the present era, the evaluation of information assets increases the need to protect them. Cybersecurity threats such as hacking, malware, and phishing attacks require businesses to adopt proactive strategies that prioritize information security. However, security measures alone cannot provide complete protection, and to reduce the risk of human error or negligence, employee education and training programs are also necessary. The benefits of effective information security are numerous, including protecting the company's reputation, complying with legal requirements, and mitigating financial losses resulting from information breaches. Therefore, companies must prioritize information security as a fundamental aspect of their business activities and continuously evaluate and update security measures to eliminate new threats and vulnerabilities.

The failure to protect the company's information assets or the inadequate implementation of security measures can lead to serious consequences, the most important of which are as follows:

1) When information sources are not adequately protected, the risk of information loss increases. This can result in the loss or theft of important information such as customer data, financial information, and other sensitive data.

2) The disruption or complete cessation of business processes can occur as a result of data breaches or attacks. This can lead to critical activities being disrupted, such as customer service, production, sales, and financial operations.

3) The loss or breach of information security may result in financial losses for the company. For instance, significant amounts of money may be required for information recovery or system reinstallation.

Conclusion

Due to several reasons mentioned above, it is extremely crucial for a company to protect its information reserves. To mitigate these risks and safeguard all organizational information, information security policies and security measures must be implemented. As it appears, every hazard has its own various consequences. However, technologies are constantly being developed and prepared to eliminate these damages.

References

[1] https://techvera.com/4-ways-to-protect-your-business-information-and-data/
[2]https://www.travelers.com/resources/business-topics/cyber-security/5-ways-to-help-protect-company-data
[3] https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/
[4]https://tr.linkedin.com/pulse/simmetrik-və-asimmetrik-şifrələmə-https-qoşulma-man-murad-adigozelov
[5] https://www.fcc.gov/communications-business-opportunities/cybersecuritysmallbusinesses
[6] https://arsenalfire.az/mhsullar/giri-nzart-sistemlri.html
[7] http://www.sciencecert.az/secpolicy.html
[8] https://qafqazinfo.az/news/detail/sirketler-ucun-daxili-nezaret-sistemfoncolorredtehlilfont-30859