Methods of creating information security in enterprises

Yagub Sardarov, Nergiz Aliyeva

Abstract

Information security is the measures taken to protect against risks related to the use, collection, processing, transmission and storage of information. It ensures the protection of all kinds of information such as personal data, bank accounts, customer base, business data, medical data. Information security issues are one of the main problems of today's information technologies. This issue is given importance all over the world and many standards and measures are applied to protect information. These measures include technology measures such as encryption, network security, antivirus programs, firewalls and data backups to protect data. In addition, companies and organizations should adopt a policy focused on information security and instruct their employees on information security. Maintaining information security is basically about manually processing information and maintaining control over information for its accuracy and confidentiality. As a guarantee of information security, necessary measures should be taken to protect any information itself. If these precautions are not taken, the information remains unprotected and possible risks arise. With the development of information technologies, the increase in information security is also increasing. This gives us more security features, more technological measures and more secure information.

Key words: Collection, processing, transmission, personal data, bank accounts, customer base.

Information security is the process of protecting information stored and managed in electronic and physical form and protecting it from illegal, malicious or unwanted use. This process ensures confidentiality, accuracy and positivity of data.Data security is a very important issue in today's technology and information age. The ubiquity of the Internet makes it easy for users to store and send information online. However, this creates many risks based on data security.There are some basic principles for ensuring data security. These include principles such as confidentiality, truthfulness, positivity, reduction of confusion, and trustworthiness. These principles play an important role in protecting against confidential and illegal use of data and ensuring that data is complete and accurate.Some measures should be taken to ensure data security.

These include measures such as encryption, password protection, data protection against illegal and malicious use, and data backup.Recently, the issue of data security has become even more important because many network security systems are poorly constructed and can pose serious threats to data. For this reason, understanding the importance of information security and developing these principles, taking certain measures and securely managing information are very important in today's information age.

The following methods can be used to ensure the information security of an institution:

Policies and Procedures: It is important for organizations to establish and implement policies and procedures to ensure information security. These policies and procedures can help create information security awareness among employees and strengthen the organization's information security culture.

Training and Awareness: Organizations should invest in regular training programs to educate and raise awareness of their employees on information security.

These trainings ensure that employees are informed about issues such as recognizing information security risks, creating secure passwords, and recognizing social engineering attacks.Data Security and Encryption: Organizations should use appropriate technologies to encrypt and protect sensitive information. The security of data can be provided with solutions such as encryption and database security technologies.

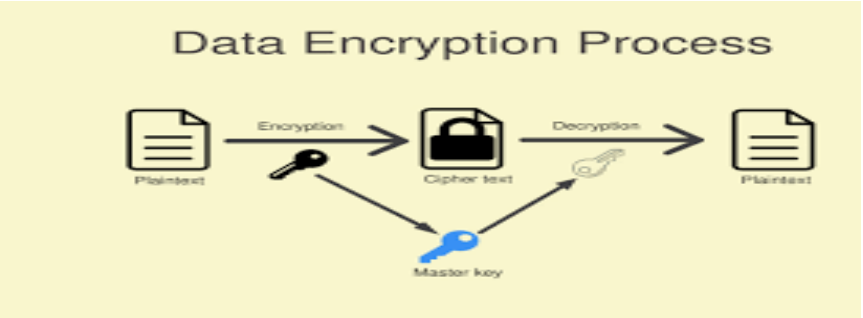

Figure 1. Data Encryption Process

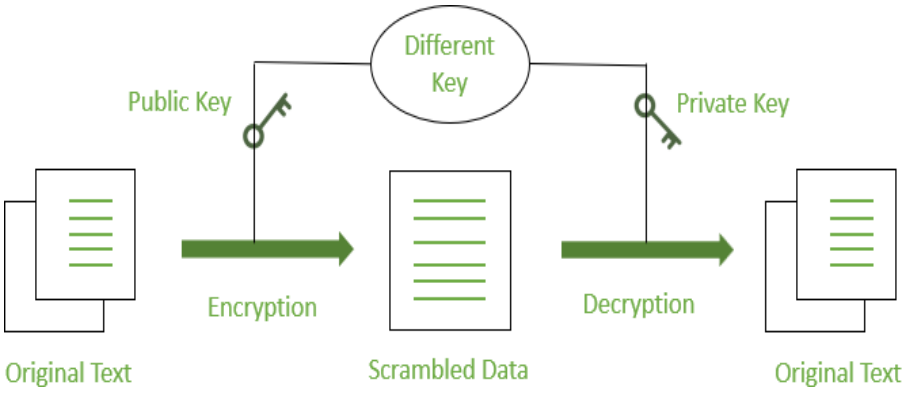

Figure 2. Data Encryption

Information encryption is the process of encrypting a message, data, or file in a way that is difficult to understand. This process allows only the message encrypted with the correct key to be understood and prevents unauthorized persons from reading the content of the message.

Information encryption consists of three main steps:

1. Encryption: The process of encrypting the message or data. In this step, the message is converted to a different form from its original state and encrypted in a way that is difficult to understand.
2. Key generation: The correct key must be generated before the encrypted message can be decrypted. The key is used to reverse the encryption.
3. Decryption: The process of converting the encrypted message to its original form using the correct key. In this step, the encrypted message is decrypted and made original.Information password is used in many fields. It is especially used in sensitive areas such as communication on the internet, banking and health sectors. In these areas, encryption of information is vital to the privacy and security of customer information.

Information encryption methods include symmetric-key encryption and asymmetric-key encryption. Both methods encrypt messages using different keys, but in asymmetric-key encryption, different keys are used while in symmetric-key encryption, the same key is used. Asymmetric-key encryption is considered a more secure method, but requires a slower processing time.

Up-to-Date Software and Patch Applications: Establishments should ensure that up-to-date software and patch applications are used in computer and network systems. This increases the security of systems and minimizes potential vulnerabilities.

Physical Security: Information security has not only a digital aspect, but also a physical aspect. Organizations should take the necessary measures to control physical access to computer systems and data centers and to ensure security.
Audit and Monitoring: Institutions should perform auditing and monitoring to reduce information security risks. These processes can control the efficiency and security of the systems, thereby making the organization more secure in terms of information security. The use of these methods enables organizations to be in a stronger position in terms of information security. However, it is not enough to use a set of methods for information security. Organizations should constantly monitor risks, update their information security policies and procedures, and regularly train and raise awareness of their employees.
As it can seen, information is used in enterprises, as well as on a wide scale of the market of information services. The protection of that information is necessary. The main reason for the problems in ensuring security is the lack of a well thought out or approved policy to ensure security. The main reasons for the loss of information privacy are disclosure, information leakage,unauthorized access. In addition, the measures performed during security and the main nuances in the implementation of those measures were determined.Measures taken by banks to address the danger of information may include:
Strict Data Security Policies: Banks implement strict policies for the security of sensitive data. These policies provide a comprehensive framework for storing, sharing and accessing data.
trict Authentication and Access Controls: Banks apply strict authentication and access controls for the security of customer information. This ensures that only authorized persons can access customer data and prevents unauthorized access.
Current Software and Patch Applications: Banks ensure the use of up-to-date software and patch applications on computer systems. This increases the security of computer systems and minimizes potential vulnerabilities.
Continuous Monitoring and Threat Monitoring: Banks detect cyber attacks in advance by using continuous monitoring and threat monitoring systems. These systems minimize the bank's information security risks by monitoring potential threats.
Training and Awareness: Banks invest in regular training programs to educate and raise awareness of their employees on information security. These trainings help bank employees recognize information security risks and increase the security of customer information.
Strict Physical Security: Banks take the necessary measures to control physical access to computer systems and data centers and to ensure security.
Emergency Preparedness: Banks prepare contingency plans to be prepared for emergencies such as cyber attacks or natural disasters.

Conclusion

As can be seen from the researches, information security is a topic that should be given a lot of attention today. Information security is a set of processes that protect the information environment of enterprises from both internal and external threats. Experience also shows that the information security system of most enterprises is not designed correctly. This, of course, may lead to the loss of information in those enterprises or leakage to external sources in the future. Here, the main responsibility falls on the employees, so employees should have information about how to deal with the obtained information, rules for using the Internet, etc.

References

[1] Hackers Attack Every 39 Seconds, 2017. URL:https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.
[2] Overview: 30 Small Business Cyber Security Statistics, 2020. URL:
Https://www.fundera.com/resources/small-business-cyber-security-statistics.
[3] Nicodemus, Report: Average data breach costs public companies $116, 2020. URL:

Https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-publiccompanies-116m/29037.article.
[4] O. Baranovsky, Financial Security in Ukraine (Assessment Methodology and Mechanism of Security Provision): Monograph, Kyiv, KNTEU, 2014, 759 p.
[5] G.V. Solomina, Ensuring Financial and Economic Security of the Enterprise: Tutorial, Dniepr, Dnipropetrovsk State University of Internal Affairs, 2018, 234 p.
[6] https://security.calpoly.edu/content/practices/good_practices
[7] https://blog.bismart.com/en/how-to-use-these-most-effective-data-security-techniques
[8] https://duo.com/blog/10-basic-information-security-practices