Project:

STUDY CONTROL SYSTEM FOR UNIVERSITIES
DIPLOMADA#1100266
MILESTONE 2 COMPLIANCE REPORT
Implementation of security measures: authentication, authorization and encryption

In addition to the security, immutability and encryption protocol offered by the Cardano Blockchain; DIPLOMADA contain security measures such as authentication, authorization and encryption, essential to protect sensitive information and guarantee the integrity, confidentiality and availability of data. Each of these measures are detailed below:

1. AUTHENTICATION:

- Authentication is the process by which the identity of a user or system is verified before allowing access to protected resources.

- These common authentication practices include:

- Strong passwords: DIPLOMADA recommends the use of complex passwords that include lowercase and uppercase letters, numbers and special characters.

- Two-factor authentication (2FA): An additional layer of security will be added to require a second authentication method, such as a code sent to a mobile device or user's email. (Not developed in this MVP).

- Biometric authentication: To comply with international standards against money laundering, due diligence and the KYC method, DIPLOMADA will use authentication methods with unique physical characteristics of the user, such as fingerprints or facial recognition. (Not developed in this MVP).

In the DIPLOMADA application, strong passwords are used and in the near future two-factor authentication will be used, which is more robust. The keys are stored in MD5 format in the typical LINUX /etc directories.

2. AUTHORIZATION:

- Authorization determines the permissions and privileges that a user or system has once they have been authenticated. DIPLOMADA you have an authorization scheme by user role.

- Some common authorization practices include:

- Principle of least privilege: DIPLOMADA includes a scheme that grants users only the permissions necessary to perform their tasks, thus avoiding excess privileges and verifying that each user role only has access to the assigned modules.

Access audit: Records and monitors user activities to detect possible unauthorized access. Logs play a fundamental role in providing a window into the activity of systems, applications and services, also known as logs, are detailed records of events that They occur in a system that will allow us to: (Not developed in this MVP)

1.- Problem diagnosis: They act as a crucial diagnostic tool. When problems or errors arise, logs allow system administrators to trace and understand the sequence of events that led to the problematic situation.

2.- Audit and compliance: They also play a crucial role in audits and regulatory compliance. They record system activities, which is essential to demonstrate compliance with regulations and policies.

3.- Activity monitoring: They monitor and record the activities carried out by users and systems. This may include accesses, configuration changes and transactions, among other relevant events.

4.- Security and intrusion detection: Logs are a valuable tool for security. They can be used to detect unusual patterns or malicious activity that could indicate intrusion attempts.

5.- Performance optimization: Analyzing them also allows you to optimize the performance of systems and applications. By understanding how resources are used and identifying potential bottlenecks, operations teams can improve efficiency and responsiveness.

3. ENCRYPTION:

- Encryption consists of transforming information into an unreadable format to protect it from unauthorized access.

- Some common encryption practices include:

- Encryption of data at rest: Our database manager protects data stored on devices or servers using cryptographic algorithms. PostgreSQL has the ability to use third-party keystores with a complete PKI infrastructure that allows management and encryption of centralized keys, Public key infrastructure (PKI) provides a way to verify the identity of a remote site using a digital certificate. PKI uses a certification authority (CA) to validate the information and sign it with a digital signature so that neither your information nor the signature can be modified.

- Encryption of data in transit: Protects communication between systems through secure protocols such as HTTPS. (Indicate if the current version of DIPLOM~~A~~D~~A~~ has an SSL or TLS certificate).
- Key management: Ensures the security of the keys used to encrypt and decrypt data, including their secure storage and periodic rotation.

PostgreSQL has up to 6 levels of encryption supported by the database software:

Password encryption:

Before being sent to the server, the PostgreSQL client will encrypt the user's password before storing it within the database. This means that the plaintext password is never stored on the server, making it very difficult for a potential attacker to obtain it.

Encryption for specific columns:

The pgcrypto module contains cryptographic functions to encrypt data stored in specific columns of the database. To decrypt the data, the client must send the key, and the data is decrypted on the server side.

Encryption of data partitions:

This method does not refer specifically to PostgreSQL, but rather refers to the underlying operating system that uses encryption when writing data to disk. This means that the PostgreSQL server has drive-level encryption to prevent someone from being able to read the data if they have access physical to the server.

Data encryption over a network:

It encompasses the different methods in which PostgreSQL can be configured to transfer data securely over the network. Both SSL and GSSAPI can be configured in the pg_hba.conf by specifying a host and its encryption, SSH is also a protocol accepted by PostgreSQL.

SSL Host Authentication:

For this level, both the client and the server must be configured to exchange SSL certificates in an SSL/TLS handshake. Once working, this method prevents a potential attacker from impersonating the server and accessing restricted information, also known as a Man attack. -in-the-middle.

Client-side encryption:

It involves the client encrypting the data directly before sending it to the server. This means that the client must manage all the encryption and decryption on their end, but it also eliminates the possibility of a malicious administrator having the ability to read your data.

4. CONCLUSION:

Effective implementation of these security measures requires an appropriate combination of technology, policies and procedures. It is important to carry out periodic security assessments, such as penetration tests, to identify possible vulnerabilities and ensure that the measures implemented are effective in protecting information and system security.

In this project, the HTTPS protocol is used to protect data in transit. The keys used to encrypt certain specific directories within the application are also rotated