**DATA WAREHOUSE SECURITY IMPLEMENTATION**

**COMPONENTS**:

1. **Sensors and Hardware Tag** - Unique identifier and some sensor data
2. **IoT Gateways** – collect data from hardware tags and transfers to the central hub (Networking capabilities, data processing and security features)
3. **Network** – connects the IoT gateways, the central hub and other devices in the central hub
4. **Central Hub** – serves as the main data processing and storage unit for all information collected from IoT gateways (Data analysis, inventory management, Communication with other Systems)
5. **Monitoring and control system** – inter connected with central hub and network infrastructure. Oversees all security and operational aspect of the warehouse system. Provides alerts/notifications

**MONITORING AND CONTROL SYSTEM**

**CENTRAL HUB**

Containers with Digital tags

and Sensors

.

.

.

.

**SECURITY GUIDELINES:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Sub Category** | **Guideline** | **Standard** | **ID** |
| Authentication | Password Security Credentials | Determine the resistance of the application against brute force password guessing using available password dictionaries by evaluating the length, complexity, reuse, and aging requirements of passwords. | OWASP - 4.4.7 | WSTG-ATHN-07 |
| User Account | Weak or Unenforced Username Policy | Determine the structure of account names. Evaluate the application’s response to valid and invalid account names. Use different responses to valid and invalid account names to enumerate valid account names. Use account name dictionaries to enumerate valid account names. | OWASP - 4.3.5 | WSTG-IDNT-05 |
| Access control | Hardware Tag | Set container-specific bandwidth limits based on expected network traffic. | NIST - 2.4.2 |  |
| Access control | Hardware Tag | Enable self-monitoring and automatic restoration for hardware tags detecting unusual behaviors. | NIST - CP-04(05) |  |
| Network Traffic | IoT Gateways | Implement kernel-level controls on IoT gateways that notice and attenuate large amounts of uploaded traffic from hardware tags. | NIST - 2.4.2 |  |
| Firewall | Access | Define concise policies for firewall rules and basic network access in the warehouse. Provide visual representations for easy understanding. | NIST - Best Practice |  |
| Access control | IoT Devices | Implement strict access controls for IoT devices.  Establish an incident response plan with defined roles and responsibilities. | OWASP - 4.3.1 | WSTG-IDNT-01 |
| Data Encryption | Sensitive Data | Implement data encryption measures to protect sensitive information. Utilize strong encryption algorithms (e.g., AES, RSA). Apply encryption at rest and segment encryption based on data nature and criticality. | OWASP - 4.9.4 | WSTG-CRYP-04 |
| Wireless Communication | Security | Utilize strong encryption for wireless communication. Implement frequency hopping or spread spectrum techniques. Deploy Wireless Intrusion Detection Systems (WIDS) to detect and respond to unauthorized activities. Implement physical security measures and network segmentation. | NIST - AC-18 W |  |
| Integrity Check | Business Logic | Review the project documentation for components of the system that move, store, or handle data. Determine what type of data is logically acceptable by the component and what types the system should guard against. Determine who should be allowed to modify or read that data in each component. Attempt to insert, update, or delete data values used by each component that should not be allowed per the business logic workflow. | OWASP - 4.10.3 | WSTG-BUSL-03 |
| Cloud Storage | Access control | Assess that the access control configuration for the storage services is properly in place. First, identify the URL to access the data in the storage service, and then consider the following tests:  read unauthorized data upload a new arbitrary file | OWASP - 4.2.11 | WSTG-CONF-11 |
| HTTP methods |  | Enumerate supported HTTP methods. Test for access control bypass. Test HTTP method overriding technique | OWASP - 4.7.3 | WSTG-CONF-06 |
| Application misuse | Identifying vulnerabilities | Generate notes from all tests conducted against the system. Review which tests had a different functionality based on aggressive input. Understand the defenses in place and verify if they are enough to protect the system against bypassing techniques. | OWASP - 4.10.7 | WSTG-BUSL-07 |
| Network Infrastructure Configuration | Security and Configuration | Review the applications’ configurations set across the network and validate that they are not vulnerable. Validate that used frameworks and systems are secure and not susceptible to known vulnerabilities due to unmaintained software or default settings and credentials. | OWASP - 4.2.1 | WSTG-CONF-01 |

**s**