Network and Data Security Report for MAISON

Rohan Shah

9/18/2024

1. Executive Summary

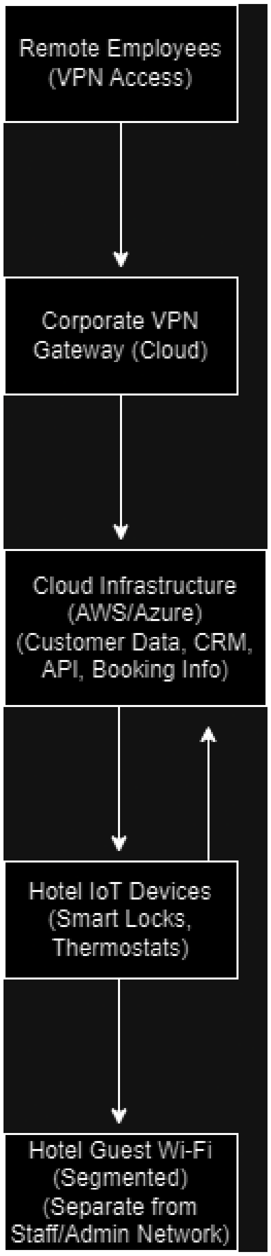
This report analyzes the network and data security architecture for MAISON, a digital-first hotel startup. The focus is on protecting the network and data infrastructure against potential vulnerabilities such as unauthorized access, data breaches, and system disruptions. Solutions such as segmentation, encryption, and continuous monitoring are recommended to strengthen MAISON's cybersecurity posture.

2. Data & Network Architecture

MAISON's network infrastructure is built to support its remote workforce, cloud storage, and smart IoT devices in hotels. Below is an outline of the key components:

- **Cloud Infrastructure (AWS/Azure)**: Used to store customer and booking data, manage CRM, and handle API communications.
- **Corporate Network (Remote Employees)**: VPN connections and secure gateways allow MAISON's employees to access the cloud and CRM from remote locations.
- **Hotel Wi-Fi**: A segmented guest network and an internal staff network ensure separate traffic flows between customer devices and hotel management systems.
- **IoT Devices (Smart Locks, Thermostats)**: These devices communicate securely with the cloud server for room access and management.
- **Third-Party Integrations**: API connections with third-party vendors like car rental companies to provide a seamless customer experience.

Network Topology Diagram


Remote Employees (VPN Access)
Corporate VPN Gateway (Cloud)
Cloud Infrastructure (AWS/Azure) (Customer Data, CRM, API, Booking Info)
Hotel IoT Devices (Smart Locks, Thermostats)
Hotel Guest Wi-Fi (Segmented) (Separate from Staff/Admin Network)

Key Components:

1. Remote employees access the cloud securely via a VPN.

2. Cloud Infrastructure stores and processes guest and booking information.

3. IoT devices at hotels connect to the cloud to manage guest access.

4. Guest Wi-Fi is separated from the internal staff network for security.

3. Security Concerns

Several security risks are associated with the network architecture:

- **Data Breach**: A breach in the cloud infrastructure could expose sensitive guest information (e.g., payment data, personal info).
- **Man-in-the-Middle Attacks (MITM)**: Communication between IoT devices (smart locks) and the cloud could be intercepted if not properly encrypted.
- **Unsecured APIs**: Third-party integrations with car rental companies and other services can introduce vulnerabilities if API communications are insecure.
- **Denial of Service (DoS)**: The guest booking system and IoT devices could be targeted with DoS attacks, potentially disrupting hotel operations.
- **Wi-Fi Network Vulnerabilities**: The guest Wi-Fi network could be a vector for attacks if not properly segmented and secured.

4. Process-Driven Security Solutions

To address these security concerns, several process-driven solutions are recommended:

1. **Network Segmentation**:
   - Segment the **guest Wi-Fi** network from the **internal staff network** to reduce the risk of lateral movement from compromised guest devices to critical hotel systems.
   - Implement **virtual LANs (VLANs)** to further isolate traffic between different segments of the network.
2. **Encryption**:
   - Encrypt all data transmitted between **IoT devices** and the cloud infrastructure using **TLS 1.3**.
   - Ensure that sensitive customer data is encrypted at rest in the cloud using **AES-256**.
3. **Vulnerability Management**:
   - Perform regular **vulnerability scans** on the network infrastructure and cloud services to identify and patch security weaknesses.
   - Regularly update **firmware** on IoT devices to prevent vulnerabilities from being exploited.
4. **Penetration Testing**:
   - Conduct **penetration tests** on the network, especially on the cloud APIs and IoT devices, to identify potential security holes.
   - Test the **availability** of the booking system and critical IoT devices under stress to evaluate resistance against DoS attacks.

5. **Logging & Monitoring**:
    - Implement **real-time log monitoring** for critical components such as cloud servers, IoT devices, and employee access via VPN.
    - Use a **Security Information and Event Management (SIEM)** system to collect, analyze, and respond to security events.
6. **Threat Intelligence**:
    - Leverage **threat intelligence** platforms to stay updated on emerging vulnerabilities in cloud services and IoT devices.
    - Monitor the security of **third-party APIs** to prevent insecure integrations from introducing vulnerabilities.

5. Recommendations

To enhance MAISON's overall network and data security, the following recommendations should be implemented:

- **Network Segmentation**: Ensure robust segmentation between the guest network and internal hotel systems.
- **Secure API Integrations**: Use secure authentication methods like **OAuth2.0** for all API communications between third-party vendors and the cloud infrastructure.
- **Data Encryption**: Ensure that all sensitive guest data is encrypted both in transit and at rest, using industry-standard encryption algorithms.
- **Zero Trust Architecture**: Consider adopting a **Zero Trust** security model, where all network traffic is authenticated and verified before access is granted.

6. Conclusion

MAISON's reliance on cloud-based infrastructure, IoT devices, and third-party integrations requires a robust network and data security strategy. By implementing solutions such as network segmentation, encryption, vulnerability management, and continuous monitoring, MAISON can protect against a range of potential threats, including data breaches, DoS attacks, and insecure APIs. With these measures in place, MAISON will strengthen its cybersecurity posture, ensuring that both guest data and critical hotel operations remain secure.