Cybersecurity Risk Assessment

Rohan Shah

9/18/2024

1.1. Introduction

In the digital-first hotel startup landscape, MAISON faces unique cybersecurity challenges due to its reliance on cloud infrastructure and interconnected digital services (e.g., online booking, smart room access). A thorough risk assessment is essential to ensure the protection of customer data, safeguard operations, and ensure regulatory compliance.

1.2. Processes Description

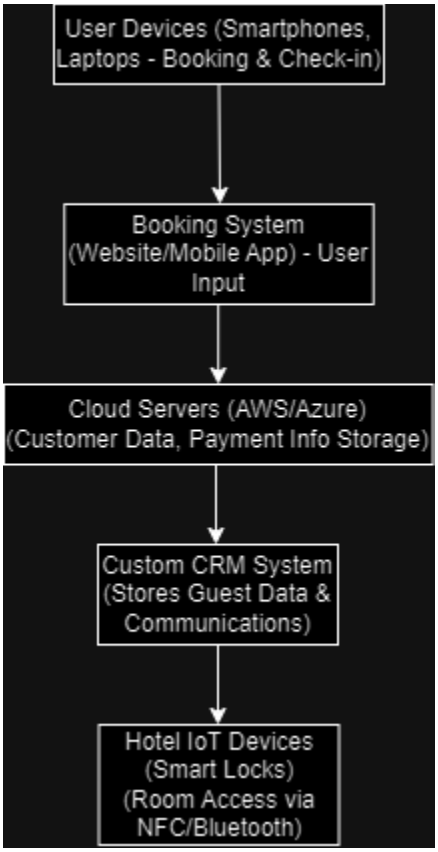
Booking Process:

- **User Interaction**: Customers input their details (name, payment information, etc.) into MAISON's app/website.
- **Data Transmission**: Data is encrypted and sent to a cloud server (AWS/Azure).
- **Storage**: Sensitive information such as payment details are stored using encryption standards (e.g., AES-256).
- **Data Retrieval**: APIs are used to retrieve booking details.

Check-in Process:

- **Smartphone Interaction**: Upon arrival, customers can check in using the app, which communicates with the smart lock on the room door via NFC or Bluetooth.
- **Access Tokens**: The app receives a temporary token from the cloud server, enabling room access.
- **Communication**: Communication with the cloud is over TLS to prevent eavesdropping.

1.3. Data Flow Diagram



Data Flow:

1. User Devices send booking info to the Booking System.

2. Booking System transmits encrypted data to Cloud Servers.

3. Cloud Servers store the data and communicate with CRM for guest profiles.

4. Hotel IoT devices (Smart Locks) interact with Cloud Servers for room access.

Security Considerations:

- Ensure end-to-end encryption between User Devices and Cloud Servers.
- API authentication between Cloud Servers, CRM, and IoT devices.
- Data encryption at rest on Cloud Servers.

1.4. Risk Identification

Using both qualitative and quantitative methods, we can break down risks as follows:

Data Breach: Unauthorized access to sensitive data.

- **Likelihood**: Medium
- **Impact**: High (financial and reputational damage)
- **Mitigation**: Data encryption, access controls, regular audits.

Man-in-the-Middle Attack: Attackers intercept communication between the app and the server.

- **Likelihood**: Medium
- **Impact**: High
- **Mitigation**: End-to-end encryption, public key infrastructure (PKI).

Outdated SSL/TLS Certificates: These can expose communication between clients and servers.

- **Likelihood**: Low
- **Impact**: High
- **Mitigation**: Automating certificate renewal processes, using HTTPS Strict Transport Security (HSTS).

1.5. Risk Register and Assessment

Risk	Likelihood	Impact	Mitigation
Data Breach	High	Severe	Encryption at rest and transit, encryption key rotation, access control
Man-in-the-Middle Attack	Medium	High	Implementing mutual TLS, Wi-Fi encryption
Phishing Attack	Medium	Moderate	Employee training programs, two-factor authentication (2FA)
API Exploit	Medium	High	API gateway security, OAuth2, API input validation
Ransomware on Hotel Management System	Low	Severe	Regular backups, strong access policies, endpoint detection and response

1.6. Analysis and Recommendations

- **Encryption**: Continue using encryption at rest and in transit. Consider upgrading to quantum-resistant algorithms for future-proofing.

- **Regular Audits**: Conduct penetration testing to evaluate any weak spots in API and system design.
- **Employee Training**: Focus on phishing simulations and cybersecurity awareness for staff, reducing the likelihood of social engineering attacks.

1.7. Conclusion

A well-executed cybersecurity risk assessment forms the foundation of MAISON's data protection strategies. The analysis has shown critical points that need continuous monitoring and improvement, especially around data breaches and communication channels.