MAISON CYBERSECURITY CAPSTONE PROJECT

Executive Presentation by Rohan Shah

9/18/2024

INTRODUCTION

Objective: To outline the key cybersecurity measures, business continuity strategies, and incident response frameworks developed for MAISON, ensuring resilience and security for critical business operations.

Context: MAISON, a digital-first hotel startup, relies on cloud infrastructure, IoT devices, and third-party integrations, making cybersecurity and business continuity essential.

CYBERSECURITY RISK ASSESSMENT

Key Processes: Booking system and digital check-in/check-out processes.

Risks Identified:

- Data breaches (customer information, payment data).
- Unauthorized access to IoT devices.
- API vulnerabilities in third-party integrations.

Recommendations:

- Encryption of data at rest and in transit.
- Multi-factor authentication (MFA).
- Regular vulnerability scanning and penetration testing.

THREAT MODELING (STRIDE)

Threats Identified:

- Spoofing (impersonating users).
- Tampering (modifying booking data).
- Information disclosure (exposed APIs).
- Elevation of privilege (unauthorized admin access).

Controls:

Strong API security with OAuth2.0.

Regular system audits and access control reviews.

Real-time monitoring and alerts (SIEM tools).

NETWORK AND DATA SECURITY

Network Topology: Cloud-based infrastructure, segmented guest and staff networks, secure IoT devices.

Key Concerns:

- Data breaches via cloud misconfigurations.
- Man-in-the-middle attacks on IoT communication.
- DoS attacks on booking services.

Solutions:

- Network segmentation and VLANs.
- Secure API integration with third-party vendors.
- SIEM and EDR tools for monitoring and rapid response.

THIRD-PARTY RISK MANAGEMENT

Vendors and Risks:

- Cloud providers, payment processors, car rental API integrations.
- API vulnerabilities, data mismanagement, compliance risks (PCI-DSS, GDPR).

Shared Responsibility Model:

- Clear delineation between vendor responsibilities and MAISON's internal security obligations.

Risk Mitigation:

- Vendor assessments, API security best practices, regular audits, and contractual clauses for data protection.

INCIDENT RESPONSE PLAN (NIST)

Incident Handling Phases:

- **Preparation**: Employee training, security policies, tools like SIEM and EDR.
- **Detection & Analysis**: Monitoring, identifying indicators of compromise (IoCs).
- **Containment**: Short-term system isolation, long-term patching and fixes.
- **Eradication**: Removal of malware, addressing root causes.
- **Recovery**: System restoration, testing, and validating data integrity.

Key Tools: SIEM (Splunk), EDR (CrowdStrike), forensic tools (EnCase).

BUSINESS CONTINUITY PLAN (BCP)

Critical Systems: Cloud-hosted booking platform, IoT devices, third-party APIs.

BCP Phases:

- **Preparation**: Regular testing and simulations.
- **Response**: Immediate activation of the BCP after system disruptions.
- **Recovery**: Restoration of critical services, data validation, functional testing.

Roles and Responsibilities:

- Business Continuity Manager, IT/Security Team, Operations, and Communications.

Task/Activity	Business Continuity Manager	IT and Security Team	Operations Team	Communication Lead	Senior Management	Third-Party Vendors
Plan Activation	A	R	C	I	I	I
Notify Stakeholders	A	R	C	R	I	I
Outage Assessment	R	R	C	I	A	I
System Isolation/Containment	I	A	I	I	C	I
Cloud System Recovery	C	A	I	I	C	R
IoT Device Recovery	C	A	I	I	C	R
Communication to Customers	I	I	I	A	C	I
Third-Party Integration Recovery	I	C	I	I	C	A
Sequence of Recovery Activities	A	R	I	I	C	I
Recovery Testing	R	A	R	I	I	I
Recovery Declaration	A	C	I	I	C	I
Post-Incident Review	A	C	C	I	R	I

IMPACT AND RECOMMENDATIONS

Business Impact:

- Cybersecurity measures will reduce the likelihood of costly breaches and protect customer trust.
- Efficient business continuity processes will minimize downtime during disruptions.

Strategic Recommendations:

- Adopt a **Zero Trust** security model.
- Conduct regular **penetration testing** and vendor security assessments.
- Strengthen API security with more granular access controls and monitoring.
- Regular **staff training** to improve incident detection and response.

CONCLUSION

Key Takeaways:

- MAISON's cybersecurity and business continuity strategy ensures protection against major threats and swift recovery from incidents.
- Security measures focus on critical areas: cloud infrastructure, IoT devices, and third-party APIs.
- With regular testing and adherence to these plans, MAISON can sustain operations securely and efficiently in the face of future disruptions.

THANK YOU

Q & A