Incident Response Plan for MAISON

Rohan Shah

9/18/2024

1. Purpose & Scope

The **purpose** of this Incident Response Plan (IRP) is to establish a structured process for responding to cybersecurity incidents that may affect MAISON's digital-first hotel operations, cloud infrastructure, and IoT devices. The plan ensures that the organization can identify, mitigate, and recover from incidents with minimal disruption while protecting sensitive customer data.

Scope:

- This IRP covers all systems and components of MAISON's infrastructure, including:
  - Cloud systems (AWS/Azure) hosting guest and booking data.
  - IoT devices (smart locks, thermostats) in hotel locations.
  - Third-party integrations (e.g., car rental API).
  - Payment processing systems.
  - Corporate networks accessed by remote employees.

2. Authority

The Incident Response Plan is authorized and enforced by MAISON's senior management and legal team. The **Cyber Security Incident Response Team (CSIRT)** has the authority to execute all aspects of this plan, including isolation of systems, user access revocations, and communication with third-party vendors and law enforcement when necessary. All actions taken by the CSIRT must be reported to senior leadership for further review.

3. Definitions

- **Cybersecurity Incident**: Any event that may compromise the confidentiality, integrity, or availability of MAISON's systems, networks, or data.
- **Breach**: A confirmed incident where unauthorized access to MAISON's sensitive data has occurred.
- **Incident Response Team (IRT)**: A group of trained professionals responsible for handling cybersecurity incidents.
- **Indicators of Compromise (IoCs)**: Data points (e.g., abnormal login behavior, unusual traffic spikes) that may suggest a security incident.
- **Containment**: Actions taken to limit the scope and impact of an ongoing incident.

- **Eradication**: Removing the root cause of a cybersecurity incident (e.g., malware, vulnerabilities).
- **Recovery**: Restoring systems to normal operation after an incident.

4. How To Recognize A Cyber Incident

Cyber incidents can be recognized by a combination of tools, alerts, and human reports. Indicators of compromise (IoCs) that may suggest a cybersecurity incident include:

- **Unusual Login Activity**: Multiple failed login attempts, especially from unknown or geographically unusual IP addresses.
- **Data Exfiltration**: Unusual amounts of data leaving the network, indicating potential data theft.
- **Malware Alerts**: Security tools (e.g., CrowdStrike) detecting malware on endpoint devices or cloud systems.
- **IoT Device Anomalies**: Unexpected behavior from smart locks or other IoT devices, such as unauthorized access attempts.
- **System Crashes**: Frequent system crashes or network slowdowns could indicate a Denial of Service (DoS) attack.
- **API Abuse**: Suspicious activity through third-party integrations (e.g., the car rental API) that may indicate exploitation attempts.

5. Cyber Security Incident Response Team (CSIRT)

The CSIRT is responsible for coordinating and executing all aspects of the incident response. It consists of representatives from several key areas:

- **Team Leader**: Responsible for decision-making, incident management, and communication with external stakeholders (including third-party vendors and legal authorities).
- **Security Analysts**: Monitor for threats, analyze incidents, and recommend response actions.
- **IT Support**: Implement containment, eradication, and recovery procedures across cloud and IoT systems.
- **Legal Team**: Ensure that all response efforts comply with regulatory requirements (e.g., GDPR, PCI-DSS) and handle communications with law enforcement if needed.
- **Public Relations (PR)**: Manage external communications during an incident, ensuring that the company's public response is appropriate and timely.

6. Contact Information

In the event of a cybersecurity incident, the following contacts should be immediately notified:

- **CSIRT Leader**: Fkwnaa Sfasw, 6479800987, asjdoiawj@gmail.com
- **IT Security Lead**: Asaoijd Sajsd, 4167326453, doij@gmail.com
- **Cloud Service Provider Contact**: AWS Security Team, 6589308274, doiawj@gmail.com
- **Third-Party API Vendors**: Car Rental API Team, 4167389748, oiasjdoiawj@gmail.com
- **Legal Counsel**: Sadnfoe Sjdjajiw, 6478769304, dsjdoiawj@gmail.com
- **PR Contact**: Lnfodj Doeoan, 6477859076, doiasiawj@gmail.com

7. Incident Types

MAISON may face various types of cybersecurity incidents. Below are the key categories:

- **Data Breach**: Unauthorized access to or exposure of sensitive customer or corporate data.
- **Denial of Service (DoS)**: Overloading the system to disrupt services, such as customer bookings or IoT device operations.
- **Malware Infection**: The introduction of malicious software into MAISON's systems or devices.
- **Phishing/Social Engineering**: Attempts to trick employees into revealing sensitive information.
- **Insider Threat**: An internal employee or contractor misusing access to compromise data or systems.
- **IoT Device Exploit**: Exploitation of vulnerabilities in IoT devices, leading to unauthorized access or control.

8. Incident Severity Matrix

To categorize and prioritize incidents, the **Incident Severity Matrix** outlines the severity levels based on the scope and impact of an incident.

Severity	Description	Impact	Response Time
Critical	Significant data breach, major system outages, IoT device compromise	Severe impact on business	Immediate (0-1 hr)
High	Data leak affecting key systems, major API exploitation	High financial/reputational risk	High priority (1-2 hrs)
Medium	Isolated incident (e.g., minor DoS), affecting a small subset of users	Moderate operational disruption	Medium priority (2-4 hrs)
Low	Suspicious behavior (e.g., phishing attempt), no confirmed impact	Minimal risk to operations	Lower priority (4+ hrs)

9. Incident Handling Process

The following process outlines the steps taken once a cybersecurity incident is identified. Each phase corresponds to the NIST framework: Preparation, Detection, Containment, Eradication, and Recovery.

9.1. Detection & Reporting

- **Monitoring**: Tools like **SIEM (Splunk)** and **CrowdStrike EDR** continuously monitor for anomalies (e.g., unusual traffic, login attempts).
- **Reporting**: Employees are trained to report any suspicious behavior or phishing emails to the IT security team via a designated communication channel.

9.2. Containment

- **Short-Term Containment**: Isolate affected systems (e.g., CRM, IoT devices) to prevent further damage. For DoS attacks, apply rate-limiting and IP blocking at the firewall level.
- **Long-Term Containment**: Implement patches, reconfigure settings, and apply role-based access control to prevent future exploitation.

9.3. Eradication

- **Root Cause Identification**: Use forensic tools (e.g., **EnCase**) to determine how the attack occurred and eliminate malware or vulnerabilities.
- **Credential Management**: Reset passwords, revoke privileges, and implement additional layers of security such as **Multi-Factor Authentication (MFA)**.

9.4. Recovery

- **Restore Systems**: Recover compromised systems using secure backups and validate that systems are clean and functional.
- **Monitoring**: Increase monitoring after recovery to ensure that there are no residual threats or re-infections.

9.5. Post-Incident Review

- **Review Meeting**: Conduct a post-incident analysis to identify what went well and where improvements can be made.
- **Documentation**: Update the incident log with detailed reports of the breach, responses taken, and outcomes.
- **Lessons Learned**: Incorporate new strategies into MAISON's security policies to prevent future incidents.

10. Incident Specific Handling Processes

Different types of incidents require specialized response processes. Below are tailored handling procedures for key incident types:

- **Data Breach**:
  - Isolate affected databases and systems.
  - Notify relevant authorities (e.g., GDPR data protection regulators) within the required timeframe.
  - Communicate breach details to affected customers via email and other channels, adhering to compliance guidelines.
- **Denial of Service (DoS)**:
  - Apply rate-limiting and blacklist suspicious IP addresses.
  - Implement redundancy to ensure uptime and failover strategies to maintain service availability.
  - After the attack, analyze logs to determine the source and adjust firewall rules to prevent future attacks.
- **IoT Device Exploit**:
  - Disconnect compromised IoT devices (e.g., smart locks) from the network.
  - Patch device vulnerabilities and update firmware.
  - Review all IoT device access logs to determine if unauthorized access occurred.
- **Phishing/Social Engineering**:
  - Identify and isolate compromised email accounts.

- Communicate to employees to avoid interacting with suspicious emails or clicking on links.
- Train employees to recognize phishing attempts and report them promptly.

11. Testing & Review Cycle

To ensure the Incident Response Plan remains effective, MAISON will implement a regular **testing and review cycle**:

- **Biannual Testing**: Conduct incident response simulations (e.g., phishing campaigns, data breach drills) every six months to assess the preparedness of the CSIRT.
- **Post-Incident Reviews**: After each incident, review the effectiveness of the response, identify gaps, and update the IRP accordingly.
- **Continuous Improvement**: Incorporate lessons learned from real-world incidents and simulations into the plan to enhance MAISON's response capabilities.

12. References

- **NIST Cybersecurity Framework**: https://www.nist.gov/cyberframework
- **OWASP Incident Response Guide**: https://owasp.org/www-project-incident-response/
- **GDPR Data Breach Guidelines**: https://gdpr.eu/data-breach/