Owner: Will Davies
Last Updated: 13/06/24
Last Updated By: Will Davies

Incident Response Plan

1. Introduction

Purpose

The purpose of this Incident Response Plan (IRP) is to establish a structured approach for identifying, managing, and mitigating cybersecurity incidents to minimise their impact on our organisation.

Scope

This plan applies to all information systems, networks, and data owned, managed, or operated by the organisation. It covers all types of cybersecurity incidents, including but not limited to malware infections, unauthorised access, data breaches, and denial of service attacks.

Objectives

- Detect and respond to cybersecurity incidents swiftly and efficiently.
- Minimise the impact of incidents on business operations.
- Improve the security posture of the organisation through continuous learning and adaptation.

Definitions and Acronyms

- **Incident**: An event that could lead to a loss of, or disruption to the organisation's operations, services, or functions.
- **IRT**: Incident Response Team
- **MFA**: Multi-Factor Authentication

2. Incident Response Team (IRT)

Roles and Responsibilities

- **Incident Leader**: Oversees the incident response process, coordinates team activities, and makes final decisions.
- **Communications Officer**: Manages communication with internal and external stakeholders.

Contact Information

Role	Name	Contact Number	Email
Incident Leader	Will Davies	+44 7979 902431	will@getorchestra.io
Communications Officer	Hugo Lu	+44 7477 613636	hugo@getorchestra.io

3. Incident Response Lifecycle

Preparation

- Develop and maintain an incident response policy.
- Conduct regular training and awareness programs.
- Maintain an inventory of critical assets and their associated risks.
- Ensure all tools and resources required for incident response are up-to-date and accessible.

Detection and Analysis

- Monitor systems continuously using security information and system logs
- Perform initial triage to assess the severity and scope of the incident.

Containment, Eradication, and Recovery

- **Containment**: Implement short-term and long-term containment strategies to limit the incident's impact.
- **Eradication**: Remove the cause of the incident from the environment.
- **Recovery**: Restore affected systems and verify that they are operating normally.

Post-Incident Activities

- Conduct a thorough post-mortem to identify lessons learned.
- Document the incident and response activities in the post-mortem.
- Implement improvements to prevent future incidents.

4. Incident Classification

Incident Severity Levels

- **Low**: Minor incidents with little or no impact on customers.
- **Medium**: Incidents with moderate impact, requiring some intervention.
- **High**: Significant incidents affecting critical systems or data.
- **Critical**: Severe incidents causing major disruption or data loss.

Incident Types

- **Malware Infections**
- **Phishing Attacks**
- **Unauthorized Access**
- **Data Breaches**
- **Denial of Service (DoS) Attacks**
- **Insider Threats**

5. Incident Reporting and Communication

Incident Reporting Procedures

- All employees must report suspected incidents immediately to the IRT via the designated slack channel '#security'.

Internal and External Communication

- Communicate incident details to relevant internal stakeholders
- Notify external parties such as customers, partners, and regulatory bodies as required.

6. Incident Handling Procedures

Initial Response

- Verify the incident and gather preliminary information.
- Notify the Incident Leader and initiate the incident response process.

Incident Analysis and Triage

- Conduct a detailed analysis to determine the nature and scope of the incident.
- Classify the incident based on severity and impact.
- If the incident is classified as disruptive to end users notify end users using email template found in Confluence (Engineering -> Security -> Incident Response)

Evidence Collection and Preservation

- Collect and preserve all relevant evidence, following legal and regulatory requirements.

Containment Strategies

- Implement short-term containment to stop further damage.
- Develop long-term containment strategies to maintain operations while addressing the incident.

Eradication Steps

- Identify and eliminate the root cause of the incident.
- Verify that the threat has been completely removed.

Recovery Procedures

- Restore affected systems and data from backups.
- Perform thorough testing to ensure systems are secure and fully operational.

Final Steps

- Once system service is restored notify end users using email template found in Confluence (Engineering -> Security -> Incident Response)
- If possible replay events in an appropriate manner

7. Post-Mortem

- Conduct a post-mortem review meeting with all relevant stakeholders.
- Identify what worked well and what needs improvement.
- Add detail regarding what happened, why it happened, and when it happened.
- Share the report with senior management and relevant internal stakeholders.