Incident Response Plan (IRP)

Last revision date: July 30th, 2020

PURPOSE

The purpose of these procedures is to define the steps required to respond to a data security incident in Treepl CMS.

RESPONSIBLE OFFICER

Chief Infrastructure Officer

SCOPE

These procedures apply to all incidents involving information and data regardless of form that occurred within the Treepl CMS system, any of its supporting services or systems that have direct access to the backend environment.

BACKGROUND

These procedures are designed to help ensure effective and consistent data security incident response throughout Treepl CMS.

DEFINITIONS

Employees: Treepl CMS developers, project managers and system administrators.
Treepl Partners: Treepl CMS high-level resellers.
Data centers: Virtual instances managed by Treepl CMS which are used to host websites and various services.

RECOGNISING A SECURITY INCIDENT

While security incidents may not be recognised straightaway, there may be a number of indicators that employees and Partners should be aware of and be on a look out for. Such as

- A system alarm or similar indication from a antimalware software
- Unexpected changes in the server performance level (jumps in CPU, RAM, Networks usage)

- Presence of unexpected IP addresses or routing
- Suspicious entries in system or network accounting
- Sites or services going offline
- Unusual quantity of outgoing mail
- Accounting discrepancies (e.g. gaps in log-files)
- Unsuccessful logon attempts
- Unexplained, new user accounts
- Unknown or unexpected services and applications configured to launch automatically on
- System boot
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Unexplained, new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial of service or inability of one or more users to log in to an account
- System crashes
- Poor system performance
- Unauthorized operation of a program or sniffer device to capture network traffic
- Use of attack scanners, remote requests for information about systems and/or users
- Social engineering attempts
- Unusual time of usage
- Unauthorized wireless access point detected

PROCEDURES

- Any employee or Treepl Partner who suspects that a data security incident has likely occurred (or was made aware of one by a third party) shall report the incident via email to support@treepl.co

- Treepl support employees shall immediately inform the CIO and/or CTO of the incident reported.

- Unless otherwise delegated, the CIO is the Incident Commander overseeing all incident response teams and actions.
    - In the absence of the CIO, the CTO is the default Incident Commander overseeing all incident response teams and actions.

- The Incident Commander shall convene appropriate incident response teams and roles, depending on the circumstances of the incident, with the following responsibilities:
    - Incident Management Team: Treepl CMS development leaders shall direct the work of the Incident Containment Team and Incident Communications Team.

    - Incident Containment Team: Treepl CMS developers and/or system administrators appropriate to the circumstances of the incident shall work on containing the spread of damage and to the possible extent reducing or controlling existing damage.
    - Incident Communications Team: Treepl CMS development leaders and Treepl Support managers shall develop and execute communications according to the circumstances of the incident.
    - All teams under the direction of the Incident Commander shall consult with Subject Matter Experts as needed.

- The Incident Commander shall assign a severity level to the incident of High, Medium, or Low depending on the risk level of the data involved, as well as the breadth and depth of the incident and other risk factors associated with the incident.

- Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for the initial investigation into an alleged incident.

- Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for containment of a confirmed incident commensurate with the severity level and circumstances of the incident.

- Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for communication of a confirmed incident commensurate with the severity level and circumstances of the incident.

- Under the oversight of the Incident Commander, the Incident Communications Team shall report the incident and findings to Treepl Partners in Slack within 72 hours of the initial incident report.

- Under the oversight of the Incident Commander, the Incident Management team shall conduct an after-action debriefing session to evaluate the incident and the incident response for purposes of gleaning lessons learned to prevent future incidents or improve future incident responses.

- All documentation and evidence collected in response to the incident will be kept in secure storage until the Incident Commander determines it can be released.

REVISION HISTORY

Original Issuance Date: July 30th, 2020

For more information

Treepl CMS security:
treepl.co/security-overview

Treepl CMS privacy:
treepl.co/privacy-policy

Treepl CMS terms of service:
https://treepl.co/terms-of-service