INCIDENT RESPONSE PLAYBOOK

IRP # 20

LOST OR STOLEN DEVICE RESPONSE

Guidelines to handle lost or stolen device incident.

RTL

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Note: Preparation steps should primarily be completed prior to an event or incident.

- Determine the members of the Cybersecurity Incident Response Team (CSIRT).
  - The core CSIRT members should be comprised of individuals responsible for cybersecurity only.
    - This may include some members of Information Technology roles, depending on the organization size.
    - The limited size of the core CSIRT is to assist with confidentiality and efficiency.
    - The core CSIRT may be activated often to investigate security events that may or may not result in an incident.
  - Assign roles and responsibilities to each member.
- Determine extended CSIRT members.
  - This will often be Legal, Compliance, Public Relations, and Executive Leadership.
- Define escalation paths.
  - Incidents may start as events, or as a lower impact/severity and then increase as more information is gathered. Establishing an escalation path is critical to success.
- Determine controls for lost or stolen devices.
  - Remote wipe capabilities.
  - At-rest encryption.
  - Multi-Factor Authentication.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

- Identify the nature of the device that has been lost or stolen.
  - Laptop?
  - Phone?
  - Tablet?
  - Other device such as desktop, server, other equipment, etc.
- Assess the criticality of data or accounts that may be present on the device.
- Interview the user to understand the conditions around the lost or stolen device.
  - Was it misplaced?
  - Can you confirm that it was stolen?
  - Was the device logged in and active to any accounts?
- Contact local authorities to report the loss.
  - Clear this process with legal counsel first.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Disable or reset the password for any accounts that may be accessed via the lost or stolen device.
- Perform remote wipe capabilities to eradicate any sensitive data on the lost or stolen device.

ERADICATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- If the device is a laptop or other computer:
  - Disable any active directory accounts for the device.
  - Create alerts for any time the device contacts the network.
  - Disable any remote access associated with the device.
    - i.e. VPN accounts and certificates, Microsoft Intune, Exchange ActiveSync, JAMF, etc.
  - Remind user to disable or reset the password for any personal accounts in use on the device.
- If the device is a phone, tablet, or other mobile device:
  - Disable active directory accounts for the device if applicable.
  - Disable any remote access associated with the device.
    - i.e. VPN accounts and certificates, Microsoft Intune, Exchange ActiveSync, JAMF, etc.
  - Create alerts for any time the device attempts to check-in or contact the network.
  - Contact the cellular provider to notify them that the device has been lost or stolen and any associated hardware addresses should be blocked from access.
  - Remind user to disable or reset the password for any personal accounts in use on the device.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- Restore user work functionality with a trusted device.
- Create alerts for any abnormal activity from the user accounts involved.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

- Conduct a meeting after the incident to discuss the following:
  - What things went well during the investigation?
  - What things did not go well during the investigation?
  - What vulnerabilities or gaps in the organization's security status were identified?
    - How will these be remediated?
- What further steps or actions would have been helpful in preventing the incident?
- Do modifications need to be made to any of the following:
  - Remote management capabilities
  - Application security
  - Employee, IT, or CSIRT training
  - Encryption capabilities
  - Access rights to sensitive information
- Create and distribute an incident report to relevant parties.
  - A primary, and more technical, report should be completed for the CSIRT.
  - An executive summary should be completed and presented to the management team.

NEED HELP?

If you need assistance with anything in this resource, please don't hesitate to reach out to us.

CONTACT US

RTL Global SOC

soc@rtl.com