ASPIRENET LTD

Information Security

Major Incident Response Procedure

Information

Document ID	ASP-MIRP-01
Version	1.0 (Published)
Date of Version	21st July 2020
Author	Kenny McLean
Role	Cyber Security Consultant
Classification	
Next Review Date	21st July 2021

Version History

Version Number	Date	Author	Description of Change
0.1	21st July 2020	Kenny McLean	Draft
1.0	24th July 2020	Kenny McLean	Published

Abbreviations & Acronyms

Abbreviation / Acronym	Description
AV	Anti-Virus
BCDR	Business Continuity & Disaster Recovery
CD	Compact Disc
DDoS	Distributed Denial of Service
DMZ	De-Militarised Zone
DoS	Denial of Service
COLO	Colocation
HDD	Hard Disk Drive
HR	Human Resources
IRT	Incident Response Team
ISO	the International Organization for Standardization
IT	Information Technology
ITSO	IT Security Officer
NIST	National Institute of Standards and Technology
OS	Operating System
SIEM	Security information and event management
SIFT	Group of free open-source incident response and forensic tools
SIRO	Security & Information Risk Officer
SysAdmin	Systems Administrator
USB	Universal Serial Bus

Contents

1. Purpose

This document describes the necessary steps that are to be followed to ensure that the business responds appropriately to a major security incident.

2. Scope

The scope of this document applies to the *<Business Name>* owned IT infrastructure & systems, including those that are outsourced, and all individuals who can access those systems.

3. Roles & Responsibilities

The *<Business Name>* has a responsibility to clearly define and assign the roles & responsibilities required in order to successfully follow a major incident response procedure. Without clear definition and assignments of responsibilities, delays will inevitably occur during each phase of the incident response, resulting in the possible failure to resolve the incident in a timeframe acceptable to the business. The following 5 positions will be required in the event that a Major incident occurs.

3.1. Team leader

The Team Leader does not necessarily need to be technical. It should, however, be an individual within the business who has the ability to call on resources as and when required, in addition to having direct access to managers and directors of other business areas. This will assist in gaining information pertaining to the investigation within a timely manner. This position must also have the authority to permit the shutdown of assets if deemed required.

The Team Leader will oversee the incident management and prioritise the actions to be carried out during each phase of the incident response.

The following positions within the business would be suitable for this role;

- Head of Governance
- SIRO
- Service Delivery Manager
- Operations Manager

3.2. Lead Investigator

The Lead Investigator should be a technical individual capable of collating evidence and determining the root cause with the assistance of other technical individuals. The Lead Investigator should also be capable of directing recovery of affected systems.

The following positions within the business would be suitable for this role;

- ITSO
- Head of IT
- Network Manager
- Lead SysAdmin
- Senior Security Analyst

3.3. Communication Lead

The Communication Lead will be responsible for the communication and passage of information between *<Business Name>* and any outside agencies (Police, government agencies, press, 3rd party assistance etc.) that may be involved in the incident response.

The following positions within the business would be suitable for this role;

- DPO
- Head of Governance
- Head of HR
- Head of Communications

3.4. Documentation lead

The Documentation Lead is required in order to record a timeline of events. This will assist with evidence and forensics should the need arise, and also give a concise breakdown of events that occurred during the lessons learned phase of the incident response procedure.

The following positions within the business would be suitable for this role;

- HR representative
- Service Desk Representative
- Junior Security Analyst

3.5. HR/Legal Rep

An HR/Legal Representative will be required in order to give guidance in the event that an incident has occurred due to involvement by an employee, possible criminal activity, or legal/contractual obligations which may have been broken.

The following positions within the business would be suitable for this role;

- Head of HR
- Head of Legal

Beyond these 5 roles, there may be a requirement to include other personnel that have the experience and skills to assist in one or more of the phases under the Phases section below.

4. Phases

Without following a formal framework or process for incident response, the *<Business Name>* will leave itself vulnerable in the event an incident occurs. The following phases and framework are based upon ISO27035 and NIST 800-61 publications.

4.1. Preparation

The preparation phase allows the *<Business Name>* to plan for an effective incident management response and should consider the following;

Incident Response Team;

As mentioned above under the Roles & Responsibilities section, an incident response team with well-defined roles & responsibilities is required. Contact details of these assigned individuals should be listed and disseminated to all members of the team. Any changes to the roles & responsibilities should be recorded and the list amended to ensure the integrity of the list is preserved.

Policies

Policies providing a written set of principles, rules, or practices within the business, are required to give guidance as to what will be classed as an incident, what justification is required to be provided to monitor or investigate an incident, define policy violation etc.

The following policies should be considered;

- *<Business Name>* Information Security Policy
- *<Business Name>* Acceptable Usage Policy
- *<Business Name>* Audit & Logging Policy
- *<Business Name>* Security Incident and Information Loss Policy
- *<Business Name>* BCDR Policy

Communication

Clear guidance regarding communication is required to avoid any doubt surrounding who should contact outside agencies or inform the press in the event a major incident occurs. The Communication Lead should specify this guidance within *<guidance document name>*.

The *<guidance document name>* should also contain a list of contact details for those outside agencies that may be required in the event that a major incident occurs. The following agencies and businesses should be included as a minimum;

- Law Enforcement (local Police, Action Fraud)
- Information Commissioner's Office (ICO)
- 3rd party digital forensics supplier (CREST Approved)
- Cloud Incident Response Team *<if applicable>*
- COLO Provider Incident Response Team *<if applicable>*
- Contact details for *<Business Name>* remote office(s) *<if applicable>*
- Board Members & Senior Management (for escalation) *<if applicable>*

These contact details must include Out of Hours (OOH) contact details in addition to normal office hours.

Recovery Plan

A recovery plan must be established to support the Recovery/Remediation phase of this procedure. This would nominally be documented within those procedures which support the *<Business Name BCDR document name>*.

Forensic Tools

Without access to the correct forensic tools, it will be almost impossible for the first responder or on-site investigator to carry out any relevant investigative work. Therefore, it is recommended that tools, both software and hardware, be available. The following tools are suggested to be included within the incident 'Jump Bag'

- Blank external HDD's
- Write Blocker
- Redline (memory forensics)
- Wireshark (packet sniffer)
- Bootable USB/CD (various Windows & Linux OS')
- Screwdrivers, pliers etc. (for hardware removal)
- Anti-Static bags (for hardware storage)
- Forensic software installation files (e.g. EnCase)
- Dedicated laptop with virtual machines (SANS SIFT, Kali Distro, sandbox, internet access)
- Various cables & connectors (USB, Ethernet, COM port etc.)
- Digital Camera
- Evidence bags & tags

This list is not exhaustive and may be developed over time as new technologies become available and lessons learned identify tools which may have assisted the investigation.

SIEM Configuration, Logging, Monitoring

To aid in the detection and to some extent, forensic investigation, and evidence collection, a SIEM tool must be deployed. The *<Business Name>* has chosen *<Insert SIEM Tool name here>* as the SIEM tool to be used within the *<Business Name>* infrastructure. The SIEM tool must be configured to capture events from all servers and security management systems (e.g. *Web proxy, AV, Firewalls, MS Security Centre etc.)* in order that event correlation can assist in identifying threats and incidents.

User Awareness for Incident Reporting

All *<Business Name>* users must be aware of the process on how to report a security incident. This information should be disseminated regularly and when any updates are made to the reporting process. The incident reporting procedure should also include details of who an incident should be escalated to after the initial detection and incident has been logged.

Documentation

A clearly documented template should be used for all phases of a security incident. This will aid in the event capture, evidence accountability and lessons learned; the following documentation should be made available for use during a security incident;

- *<Business Name>* Security Incident and Information Loss reporting Form
- Event Logbook (Who, What, Where, When, Why & How)
- Resolution Executive Summary Document
- Security Incident Log

Training

<Business Name> should invest in training those individuals who would be involved with the investigation and forensics of a security incident. Without relevant training, the risks of incorrect handling or identification of evidence may result in the failure, or delay, of incident resolution. This

may also result in the denial of evidence submission in the event the incident requires criminal prosecution.

4.2. Identification

This phase consists of the detection, information collection, triage, reporting and the investigation of a security incident via either manual or automatic means.

Detection

The detection of a security incident may come from one or more sources. These areas may consist of one or more of the following;

- User report
- Log analysis
- SIEM alerts
- External parties

Whichever source of detection has reported the security incident, the <*Business Name*> Security Incident and Information Loss reporting Form must be completed, and an incident log generated via the IT Service Management.

Triage

Once the incident has been identified as a security incident, the severity level should be defined to determine who the incident should be reported to and if it requires escalation. The severity level will also determine the resources allocated to the incident.

Internal Reporting

Once the incident has been detected and logged, reporting the incident to the Incident Response Team (IRT) must be carried out, with minimal time disruption between the detection and reporting to the IRT. Contact details of those individuals the incident should be reported to, must be easily accessible and widely known throughout the organisation.

Information Collection

Information collected as part of the detection phase, will assist the IRT throughout the investigation in identifying systems that may be affected or the source of the cause of the incident, therefore it is vital that logs are retained for review within a centralised location. This information will also assist in identifying the type of incident, for example;

- Data Breach
- DOS/DDOS
- Data Loss
- Malware Infection
- Website Defacement
- Policy Violation
- Social Engineering
- Ransomware
- Internal Attack

By identifying the type of security incident, the IRT can determine which path to take for investigation.

Forensics & Log Analysis (Evidence gathering)

Forensic investigation and Log Analysis may be required dependent upon the type of incident that has occurred. It is therefore advised the *<Business Name>* has an individual who has some knowledge of forensic investigation and log analysis available to assist in the investigation, such as;

- Taking a copy of a hard drive
- Memory forensics
- Packet capturing
- Video/photo capture of screen activity
- System & event log capturing
- Virtualisation forensics

Anything beyond this may require 3rd party forensic/investigation service suppliers.

Who, What, Where, When, Why, How.

The who, what, where, when, why, how questions should be fundamental during the investigation and when capturing the events carried out during the investigation. These questions will assist in identifying;

- Who carried out the attack/breach (internal/external malicious individual, internal user who has accidentally carried out the breach)?
- What are they trying to achieve (steal data, install key loggers, install ransomware etc.)?
- Where is the attack happening (endpoints, servers, DMZ etc.)?
- When did the attack occur (is this a new attack or months old?)
- Why are they carrying out the attack (by knowing the motivation, it may assist in identifying other areas of the infrastructure that may be infected)
- How did the breach occur (identify the root cause in order to close it down)?

External Reporting

The decision to inform external agencies should be made, which the Communication Lead should carry out.

4.3. Containment

This phase should focus on ensuring that the breach, attack, or infection does not proliferate throughout the infrastructure and limit the damage that the attack or infection can cause.

System Changes

In order to contain the attack, breach, or infection, it may be required to carry out system(s) changes that are time constrained. In these occurrences, the Team leader should give management approval on advice from the Lead Investigator to shut down the system(s), disconnect cables, disable account(s), change password(s) etc. However, great care must be given so that the attacker is not made aware of the containment as they may try and delete evidence that could identify them.

Consideration to business users who are not affected by the incident, must also be made in the event that ad-hoc changes are needed.

The following sections highlight the stages for containment;

Short Term Containment

The initial stage to contain and limit the damage as soon as possible after identification. This could be;

- Isolating a network segment(s)
- Isolating individual system(s)
- Re-routing traffic
- Failing over system(s)

System(s) Back-up

This stage will require a forensic image of the system(s) to be taken before the system(s) are wiped for re-imaging. This will allow for the preservation of evidence as the image taken, would be that of the system(s) as they were during the incident.

4.4. Eradication

This phase will cover those stages required for the removal and restoration of the affected system(s). This phase may require repetition until all systems that have been affected have been identified, contained & the infection has been eradicated.

Backups

When re-imaging systems(s), great care must be taken to ensure that only known good images are used to back up from. Failure to do so may result in re-infection. Consideration must be taken also in the event that the affected system(s) resided on a shared host. Shared hardware resources must also be investigated for infection.

AV & Patching

Further checks should be carried out on recovered system(s) via the use of secondary AV tools that have been updated. The most recent OS and software patches should be applied prior to being connected back onto the infrastructure.

Root Cause

The root cause should have been identified, and mitigations put in place to prevent it from being exploited further. Failure to identify the root cause prior to this phase ***will*** result in re-infection.

4.5. Recovery/Remediation

This phase will enable the system(s) that were affected to be brought back into production and ensure that another incident of the same nature will occur. This phase should be carried out in conjunction with the <*Business Name*> BCDR Plan.

Test & Monitor

Monitoring of the system(s) being brought back into service is necessary to ensure that the eradication phase has been carried out successfully. Testing of the system behaviour should also be carried out to ensure that no anomalies have been introduced during the re-image/backup stages.

Documentation

At the conclusion of this phase, all documentation should be closed off, checked, and signed where required.

4.6. Lessons Learnt

This phase involves a debrief of all stakeholders affected and involved in the incident. The Security Incident Log should be completed, and the Resolution Executive Summary Document written up and disseminated to management.

The Lessons Learnt phase needs to be carried out as soon as possible after the Recovery/Remediation phase has been completed. It is suggested that this should be no longer than two weeks after the incident.

Debrief

The debrief should include a review of the Event Log Book in order to identify areas that might be open for improvement, tools that would have assisted in the identification or investigation, training gaps for those involved in the IRT and gaps within this procedure.

5. Continual Improvement

To ensure that the incident response procedure remains effective, continual improvement needs to be carried out.

5.1. Review

Regular review of this document is required to consider its applicability with new methods, technologies and frameworks that are designed for security incident management and response. The review should be carried out by those individuals who are part of the IRT.

5.2. Testing

Annual testing of the incident response procedure is required to give the business assurance that the procedure is affective and that all member of the IRT are aware of their roles and responsibilities. These tests should be catalogued and follow the phases as laid out above with particular attention the Lessons Learnt phase.