IT INCIDENT RESPONSE PLAN

Last Revision:
6/25/2020

TABLE OF CONTENTS

CHAPTER 1: Introduction

BackNine Insurance and Financial Services, Inc. is a corporation located in the state of CA. One of the most important tasks of the company is to safely secure the information of customers.

It is of great importance that an information technology (IT) incident response plan is prepared and followed by the organization in the event that there are information incidents in the organization which may hinder its normal operations.

The purpose of this plan is to describe the organization's overall plan in responding to any such incidents. The plan also provides for the roles and responsibilities of all the participants, the incidents the relationship of this plan to other policies and procedures, and the requirements for incident reporting.

The goal of this plan is to detect and react to any incident, indicate the risk of the incident, appropriately respond to the incident, communicate the process of responding to the incident to the stakeholders, and mitigate the probability of its occurrence.

With respect to the scope, this plan shall include the information systems team of the organization and all personnel having access to the systems. As provided above, it shall be the responsibility of the information security officers to maintain and make any revisions on the document.

Lastly, with regard to the maintenance and revision of this plan, the office of the CIO shall have the responsibility of doing so. As such, it shall have the authority to execute this plan, by virtue of the policy of the organization.

CHAPTER 2: Roles and Responsibilities

A. Incident Response (IR) Coordinator

The IR Coordinator is responsible for gathering all the data with respect to all the IT incident and shall have the responsibility of communicating the data to all the respective parties involved, and shall ensure that all the information gathered are true, accurate, and complete. Lastly, the IR Coordinator shall have the responsibility of communicating the status of the incident in all stages of the investigation.

The IR Coordinator of the organization is: Charles Minderhout

B. IR Handlers

The IR Handlers are responsible for gathering evidence related to the IT incident.

C. Information Technology Director

The IT Director is responsible for determining the nature and scope of the IT incident. He is also responsible for determining which member shall be included in the investigation. As the IT Director, he shall also be responsible for providing training on proper incident handling and responding. It shall also be the responsibility of the IT Director to ensure that the gathering of evidence and its preservation by the IR Handlers are done appropriately. Lastly, the IT Director shall have the responsibility of reviewing the written summary of the incident and the corrective action taken.

D. Information Technology Assistant Director

The IT Assistant Director is responsible for contacting the qualified security specialists for any needed advice with respect to the incident. He is also responsible for contacting the members of the team who shall be included in the investigation after the IT Director has determined the members. As such, he shall also assist the IT Director in providing training. Lastly, he shall prepare the written summary of the incident and the corrective action is taken and shall submit the summary to the IT Director for review.

E. Systems Administrator (SA)

The Systems Administrator has the responsibility of monitoring the business applications and services for any incident. The SA is also responsible for reviewing the contacts pertaining to the incident if requested by the IT Director. Another responsibility of the SA is to ensure that all backups are in place for all the critical systems in order to mitigate or prevent any IT incidents. Lastly, it is the responsibility of the SA to examine all the system logs of the critical systems for any unusual events or activities.

F. Network Engineer

The Network Engineer has one of the most important responsibilities in the Incident Response Team. The Network Engineer is responsible for the analysis of the network traffic for any signs of any denial of service, service traffic, or other external attacks. The Network Engineer shall also be responsible for running tracing tools in order to locate any signs of a firewall breach. He is also responsible for contacting the external service provider for any assistance in case of IT incidents. Lastly, the Network Engineer is responsible for taking the necessary action to block any unnecessary traffic from external and internal intruders.

CHAPTER 3: Methodology

The organization applies the following methodologies which shall be made as bases for the kind of response to an incident:

1. Black box Analysis Diagram

2. Tripod Beta

3. Incident Bowtie

4. Fault Tree

5. Event Tree

6. SCAT Analysis Method

Black box Analysis Diagram

The Black box analysis diagram is a method used by the organization to report smaller and lower risk incidents, in order to analyze the causes of the incidents, and to be able to determine what kind of incident response is needed to be done. This method is also used to analyze how technology, the organization, and the people have affected or played a role during the incident. Thus, this method will contain the generic cause of the incident.

Tripod Beta

This method is based on the assumption that incidents happen because organizations expose the IT systems to an imperfect working environment. Specifically, this method analyzes which barriers have been broken during the incident, the error or mistake made the working environmental aspect that encouraged the incident, and the latent failure in the organization which caused the mechanism.

Incident Bowtie

This method is a combination of the two methods provided above, which can be used to view the incident from a broader perspective in order to make sure that all the possible scenarios are taken into account in the analysis. The use of this method after the occurrence of an accident narrows down the thought process of the incident response team in order to point out all the possible scenarios.

Fault Tree

This method is used in performing reliability and safety analysis on the system, which means that this method is a deductive reasoning method for determining the causes of an incident. This method is a vertical graphics model that displays the various combinations of unwanted events which may result in the incident, and what are the options of the organization for its IT incident responses.

Event Tree

This method focuses on the events that happened prior to the incident. This method is used in order to create a holistic picture of all the risks associated with the incident, and a possible course of action for each incident. This method is used by the organization because of its simplicity.

Systematic Cause Analysis Technique (SCAT) Method

This method addresses a full range of the organization's loss of control of the events. This method is widely used for a structured analysis of incidents. Lastly, this method is used to provide the organizations with responses and actions on how to resolve the incident and to further improve.

CHAPTER 4: Types of Incidents

There are many types of IT incidents that may require the Incident Response Team's activation.

The types of incidents covered in this plan are the following:

1. Breach of personal information

2. Denial of service

3. Excessive port scans

4. Firewall breach

Breach of personal information

Breach of personal information is an incident when there is unauthorized access to the personal information of an individual that could result in harm or inconvenience to the individual. A harm that may be a risk is fraud or identity theft. The individual in this incident could either be a student or employee of the organization.

For the purpose of this plan, personal information shall include the following data:

a. Full Name

b. Age

c. Social Security Number

d. Driver's License

e. Identification Card Number

f. Financial Account Number

g. Credit or Debit Card Number

h. Home Address

i. Medical or Health Information

There may be a security breach when there is an unauthorized acquisition of data which would compromise the security, integrity, and the confidentiality of the personal information maintained by the organization.

Incident Response:

1. PREPARATION

Preparation is the key to effective incident response. In order to successfully address security events, these features will be followed:

- Develop and Document IR Policies: Establish policies, procedures, and agreements for incident response management.
- Define Communication Guidelines: Create communication standards and guidelines to enable seamless communication during and after an incident.
- Incorporate Threat Intelligence Feeds: Perform ongoing collection, analysis, and synchronization of your threat intelligence feeds.
- Conduct Cyber Hunting Exercises: Conduct operational threat hunting exercises to find incidents occurring within your environment. This allows for more proactive incident response.
- Assess Your Threat Detection Capability: Assess your current threat detection capability and update risk assessment and improvement programs. 2. DETECTION AND REPORTING

The focus of this phase is to monitor security events in order to detect, alert, and report on potential security incidents.

- Monitor: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- Detect: Detect potential security incidents by correlating alerts within a SIEM solution.
- Alert: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- Report: Your reporting process should include accommodation for regulatory reporting escalations.

3. TRIAGE AND ANALYSIS

The bulk of the effort in properly scoping and understanding the security incident takes place during this step. Resources should be utilized to collect data from tools and systems for further analysis and to identify indicators of compromise. Individuals should have in-depth skills and a detailed understanding of live system responses, digital forensics, memory analysis, and malware analysis.

As evidence is collected, analysts should focus on three primary areas:

- Endpoint Analysis
    - Determine what tracks may have been left behind by the threat actor.
    - Gather the artifacts needed to build a timeline of activities.
    - Analyze a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device.
- Binary Analysis
    - Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways.
        1. Behavioral Analysis: Execute the malicious program in a VM to monitor its behavior
        2. Static Analysis: Reverse engineer the malicious program to scope out the entire functionality.
- Enterprise Hunting
    - Analyze existing systems and event log technologies to determine the scope of compromise.
    - Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed.

4. CONTAINMENT AND NEUTRALIZATION

This is one of the most critical stages of incident response. The strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume.

- Coordinated Shutdown: Once you have identified all systems within the environment that have been compromised by a threat actor, perform a coordinated shutdown of these devices. A notification must be sent to all IR team members to ensure proper timing.
- Wipe and Rebuild: Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.
- Threat Mitigation Requests: If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication from all egress channels connected to these domains.

5. POST-INCIDENT ACTIVITY

There is more work to be done after the incident is resolved. Be sure to properly document any information that can be used to prevent similar occurrences from happening again in the future.

- Complete an Incident Report: Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future.
- Monitor Post-Incident: Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any signs of indicators tripping that may have been associated with the prior incident.
- Update Threat Intelligence: Update the organization’s threat intelligence feeds.

- Identify preventative measures: Create new security initiatives to prevent future incidents.
- Gain Cross-Functional Buy-In: Coordinating across the organization is critical to the proper implementation of new security initiatives.

Denial of service

Denial of service is an interruption of an unauthorized user’s access to a computer network, typically one caused by malicious intent. This is a cyber-attack in which the perpetrator seeks to make the network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host which is connected to the Internet. When this type of incident happens, the system of the organization which provides online service is unusable.

Incident Response:
1. PREPARATION
Preparation is the key to effective incident response. In order to successfully address security events, these features will be followed:

- Develop and Document IR Policies: Establish policies, procedures, and agreements for incident response management.
- Define Communication Guidelines: Create communication standards and guidelines to enable seamless communication during and after an incident.
- Incorporate Threat Intelligence Feeds: Perform ongoing collection, analysis, and synchronization of your threat intelligence feeds.
- Conduct Cyber Hunting Exercises: Conduct operational threat hunting exercises to find incidents occurring within your environment. This allows for more proactive incident response.
- Assess Your Threat Detection Capability: Assess your current threat detection capability and update risk assessment and improvement programs. 2. DETECTION AND REPORTING

The focus of this phase is to monitor security events in order to detect, alert, and report on potential security incidents.

- Monitor: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- Detect: Detect potential security incidents by correlating alerts within a SIEM solution.
- Alert: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- Report: Your reporting process should include accommodation for regulatory reporting escalations.

3. TRIAGE AND ANALYSIS
The bulk of the effort in properly scoping and understanding the security incident takes place during this step. Resources should be utilized to collect data from tools and systems for further analysis and to identify indicators of compromise. Individuals should have in-depth skills and a detailed understanding of live system responses, digital forensics, memory analysis, and malware analysis.
As evidence is collected, analysts should focus on three primary areas:

- Endpoint Analysis
    - Determine what tracks may have been left behind by the threat actor.
    - Gather the artifacts needed to build a timeline of activities.
    - Analyze a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device.
- Binary Analysis
    - Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways.
        1. Behavioral Analysis: Execute the malicious program in a VM to monitor its behavior
        2. Static Analysis: Reverse engineer the malicious program to scope out the entire functionality.
- Enterprise Hunting
    - Analyze existing systems and event log technologies to determine the scope of compromise.
    - Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed.

4. CONTAINMENT AND NEUTRALIZATION

This is one of the most critical stages of incident response. The strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume.

- Coordinated Shutdown: Once you have identified all systems within the environment that have been compromised by a threat actor, perform a coordinated shutdown of these devices. A notification must be sent to all IR team members to ensure proper timing.
- Wipe and Rebuild: Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.
- Threat Mitigation Requests: If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication from all egress channels connected to these domains.

5. POST-INCIDENT ACTIVITY

There is more work to be done after the incident is resolved. Be sure to properly document any information that can be used to prevent similar occurrences from happening again in the future.

- Complete an Incident Report: Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future.
- Monitor Post-Incident: Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any signs of indicators tripping that may have been associated with the prior incident.
- Update Threat Intelligence: Update the organization’s threat intelligence feeds.
- Identify preventative measures: Create new security initiatives to prevent future incidents.
- Gain Cross-Functional Buy-In: Coordinating across the organization is critical to the proper implementation of new security initiatives.

Excessive port scans

Excessive port scans, commonly known as port scan attack, occurs when an attacker sends packets to the system of the organization which results in the varying of the destination port. The attacker can use this incident to discover the kind of services that the organization is running and to get an idea of the operating system of the organization.

Incident Response:

1. PREPARATION

Preparation is the key to effective incident response. In order to successfully address security events, these features will be followed:

- Develop and Document IR Policies: Establish policies, procedures, and agreements for incident response management.
- Define Communication Guidelines: Create communication standards and guidelines to enable seamless communication during and after an incident.
- Incorporate Threat Intelligence Feeds: Perform ongoing collection, analysis, and synchronization of your threat intelligence feeds.
- Conduct Cyber Hunting Exercises: Conduct operational threat hunting exercises to find incidents occurring within your environment. This allows for more proactive incident response.
- Assess Your Threat Detection Capability: Assess your current threat detection capability and update risk assessment and improvement programs. 2. DETECTION AND REPORTING

The focus of this phase is to monitor security events in order to detect, alert, and report on potential security incidents.

- Monitor: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- Detect: Detect potential security incidents by correlating alerts within a SIEM solution.
- Alert: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- Report: Your reporting process should include accommodation for regulatory reporting escalations.

3. TRIAGE AND ANALYSIS

The bulk of the effort in properly scoping and understanding the security incident takes place during this step. Resources should be utilized to collect data from tools and systems for further analysis and to identify indicators of compromise. Individuals should have in-depth skills and a detailed understanding of live system responses, digital forensics, memory analysis, and malware analysis.

As evidence is collected, analysts should focus on three primary areas:

- Endpoint Analysis
  - Determine what tracks may have been left behind by the threat actor.
  - Gather the artifacts needed to build a timeline of activities.
  - Analyze a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device.

- Binary Analysis
    - Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways.
        1. Behavioral Analysis: Execute the malicious program in a VM to monitor its behavior
        2. Static Analysis: Reverse engineer the malicious program to scope out the entire functionality.
- Enterprise Hunting
    - Analyze existing systems and event log technologies to determine the scope of compromise.
    - Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed.

4. CONTAINMENT AND NEUTRALIZATION

This is one of the most critical stages of incident response. The strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume.

- Coordinated Shutdown: Once you have identified all systems within the environment that have been compromised by a threat actor, perform a coordinated shutdown of these devices. A notification must be sent to all IR team members to ensure proper timing.
- Wipe and Rebuild: Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.
- Threat Mitigation Requests: If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication from all egress channels connected to these domains.

5. POST-INCIDENT ACTIVITY

There is more work to be done after the incident is resolved. Be sure to properly document any information that can be used to prevent similar occurrences from happening again in the future.

- Complete an Incident Report: Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future.
- Monitor Post-Incident: Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any signs of indicators tripping that may have been associated with the prior incident.
- Update Threat Intelligence: Update the organization’s threat intelligence feeds.
- Identify preventative measures: Create new security initiatives to prevent future incidents.
- Gain Cross-Functional Buy-In: Coordinating across the organization is critical to the proper implementation of new security initiatives.

Firewall breach

Firewall breach happens when someone does not pay attention to the important logs or someone has not taken the time to analyze the security of the organization. Most often, firewall breaches arise due to configuration errors and not because of software failure.

Incident Response:

1. PREPARATION

Preparation is the key to effective incident response. In order to successfully address security events, these features will be followed:

- Develop and Document IR Policies: Establish policies, procedures, and agreements for incident response management.
- Define Communication Guidelines: Create communication standards and guidelines to enable seamless communication during and after an incident.
- Incorporate Threat Intelligence Feeds: Perform ongoing collection, analysis, and synchronization of your threat intelligence feeds.
- Conduct Cyber Hunting Exercises: Conduct operational threat hunting exercises to find incidents occurring within your environment. This allows for more proactive incident response.
- Assess Your Threat Detection Capability: Assess your current threat detection capability and update risk assessment and improvement programs. 2. DETECTION AND REPORTING

The focus of this phase is to monitor security events in order to detect, alert, and report on potential security incidents.

- Monitor: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- Detect: Detect potential security incidents by correlating alerts within a SIEM solution.
- Alert: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- Report: Your reporting process should include accommodation for regulatory reporting escalations.

3. TRIAGE AND ANALYSIS

The bulk of the effort in properly scoping and understanding the security incident takes place during this step. Resources should be utilized to collect data from tools and systems for further analysis and to identify indicators of compromise. Individuals should have in-depth skills and a detailed understanding of live system responses, digital forensics, memory analysis, and malware analysis.

As evidence is collected, analysts should focus on three primary areas:

- Endpoint Analysis
    - Determine what tracks may have been left behind by the threat actor.
    - Gather the artifacts needed to build a timeline of activities.
    - Analyze a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device.
- Binary Analysis
    - Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways.

        1. Behavioral Analysis: Execute the malicious program in a VM to monitor its behavior
        2. Static Analysis: Reverse engineer the malicious program to scope out the entire functionality.
- Enterprise Hunting
    - Analyze existing systems and event log technologies to determine the scope of compromise.
    - Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed.

4. CONTAINMENT AND NEUTRALIZATION

This is one of the most critical stages of incident response. The strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume.

- Coordinated Shutdown: Once you have identified all systems within the environment that have been compromised by a threat actor, perform a coordinated shutdown of these devices. A notification must be sent to all IR team members to ensure proper timing.
- Wipe and Rebuild: Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.
- Threat Mitigation Requests: If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication from all egress channels connected to these domains.

5. POST-INCIDENT ACTIVITY

There is more work to be done after the incident is resolved. Be sure to properly document any information that can be used to prevent similar occurrences from happening again in the future.

- Complete an Incident Report: Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future.
- Monitor Post-Incident: Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any signs of indicators tripping that may have been associated with the prior incident.
- Update Threat Intelligence: Update the organization’s threat intelligence feeds.
- Identify preventative measures: Create new security initiatives to prevent future incidents.
- Gain Cross-Functional Buy-In: Coordinating across the organization is critical to the proper implementation of new security initiatives.

CHAPTER 5: Phases of Incident Response

There are different phases to the incident response. The phases are as follows:

1. Preparation

2. Detection

3. Containment

4. Investigation

5. Remediation

6. Recovery

FIRST PHASE: Preparation

This phase includes the activities that enable the team to respond to the incident. This phase includes the preparation of the policies, tools, procedures, effective governance, as well as communication plans.

In this phase, an implication is made that the groups that are affected in the incident have made the controls which are necessary to recover and continue the operations even after the incident.

SECOND PHASE: Detection

The second phase includes the discovery of the event with security tools or given notifications within the organization or an outsourced party about any suspected incident. This phase shall also include the classification of the kind of incident.

THIRD PHASE: Containment

The second phase includes the identification of the affected system or host. This shall also be the phase where the system is isolated if needed. Aside from isolation and further mitigation, this phase shall also include the notification of the affected parties of the incident, as well as the status of the investigation.

FOURTH PHASE: Investigation

The fourth phase includes the investigation by the team in order to determine the priority, scope, and the root cause of the incident. This is one of the most important phases in the IT incident response plan because this outlines the start and end of the activities of the organization in order to address the incident.

FIFTH PHASE: Remediation

The fifth phase is the post-incident repair of any affected systems. This shall also include the communication and instruction of all the affected parties of the final status of the incident. Also, this is the phase where the confirmation is made that the incident has already been contained. It shall also be in this phase where the organization shall determine if there is a need for any regulatory requirements for the kind of incident. Lastly, this shall be the phase when all the assigned team members will prepare the reports and summaries necessary after the incident response.

SIXTH PHASE: Recovery

The last phase is the recovery. This shall be the analysis of the incident and its procedural and policy implications. It shall also be in this phase where the team shall gather the metrics and the evaluation of how the team acted on the incident response plan and whether the procedure was strictly followed.

CHAPTER 6: Guidelines

There are seven important steps which the organization may treat as guidelines in order to develop the plan which is the following:

1. Determine the authority to call an incident
2. Assign the roles and responsibilities
3. Do not assign security levels
4. Establish the communication procedures, as well as the responsibilities for each procedure
5. Gather pertinent information
6. Outline the process
7. Review and test the plan

CHAPTER 7: Documentation

All the incident response activities shall be documented in order for the organization to continuously improve its IT incident response plan.

All the incidents will be prioritized and ranked according to their potential to disclose any restricted data.

All the incidents and the incident response activities shall be reviewed after the end of every period and there shall be an assessment of whether or not the investigation process was successful and effective.

Lastly, there shall be a documentation as to whether or not there is a need for adjustments in the methods and processes that are used and applied by the team.