Automate Response

Congratulations on selecting IncidentResponse.com to retrieve your custom incident response playbook guide. This guide has been created especially for you for use in within your security response team. We hope you find it valuable and ask that you share it with the rest of your organization so you can collectively be successful in managing incidents and reducing risk throughout the business.

Your playbook overview - “Phishing”

Incident Response: A Top Priority in Security Management Programs

In the April 2014, U.S. Government Accountability Office reported (GAO-14-354) it’s noted that “major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information).” The GAO projects that these agencies did not completely document actions taken in response to detected incidents. While the agencies identified the scope of an incident, they frequently did not demonstrate that they had determined the impact of an incident, nor did they consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. The GAO notes, “without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.”

Did you know?

1. In 2014, incidents increased by 78% since 2013.¹
2. 1,023,108,627 records were breached in 2014.¹
3. 54% of the breaches consisted of Identity Theft.¹
4. $3.5 million is the average cost of a breach for a company.²
5. Companies experience an average of 10 unauthorized access incidents per month.²
6. Malicious insiders and criminal attacks are the top causes for breaches.²

1. Source: Gemalto - Breach Level Index
2. Source: Ponemon 2014 Cost of a Data Breach
3. Source: GAO-14-354, p.2
What is an incident response playbook? According to NIST Special Publication 800-61, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

**Prepare**
The initial phase where organizations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.

**Detect & Analyze**
The second phase where organizations should strive to detect and validate incidents rapidly because infections can spread through an organization within a matter of minutes. Early detection can help an organization minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains as a result of the incident.

**Contain, Eradicate & Recover**
The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organization.

**Post-Incident Handling**
Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring.

---

**Phishing**
You've selected the “Phishing” playbook. On the pages that follow, you will find your incident response playbook details broken down by the NIST incident handling categories.

To view your workflow online, visit [https://incidentresponse.com/playbooks/phishing](https://incidentresponse.com/playbooks/phishing)
PREPARE - PHISHING

1. Determine Core Ops Team & Define Roles

2. Review & Maintain Timeline

3. Interviews
   - User Manager
   - Manager
   - Physical Security
   - Key Stakeholders

4. Internal Path
   - Document

5. External Path
   - Document

Next Step
Identification of Spoofed email

Emails that have been linked to external or unknown URL's

Emails returned my mail servers as identified

Monitoring of organization websites to identify attempts or copy web content or perform web scraping

Notifications from external users or customers of suspicious or fraudulent activity related to emails

Notifications from internal users of suspicious or fraudulent activity related to emails

Notification from 3rd parties of suspicious or fraudulent activity related to emails

Notification from Law Enforcement suspicious or fraudulent activity related to emails

Notification from ISP of increased amount of email or web traffic (ingress or egress)

Identification of Spoofed email

Emails that are non-returnable or non-deliverable

Monitoring of organization websites to identify attempts or copy web content or perform web scraping

Notifications from external users or customers of suspicious or fraudulent activity related to emails

Notifications from internal users of suspicious or fraudulent activity related to emails

Notification from 3rd parties of suspicious or fraudulent activity related to emails

Notification from Law Enforcement suspicious or fraudulent activity related to emails

Notification from ISP of increased amount of email or web traffic (ingress or egress)

Categorize Incident

Request Packet Capture

Conduct Content Scans

Next Step

Detect - Phishing

Custom Indicators
ONLINE INCIDENT RESPONSE COMMUNITY

ANALYZE - PHISHING

Internal user PII or other protected information at risk of being exposed
External user PII or other protected information at risk of being exposed
PII or other protected information has been compromised
ISP and any other partners have been contacted regarding this event
Public or personnel safety affected
Customers are affected by this incident
Products/goods/services are affected by this attack
Ability to control/record/measure/track any significant amounts of inventory/products/cash/revenue has been lost
Worst-case business impact if unable to mitigate this attack
This act is being launched by known entities
There is internal knowledge of this incident
This act could be exploited for criminal activity
There is external knowledge of this incident

Standard
Define Risk Factors
Custom
Custom Factors

Determine Patch Methods
Log Collection
Evidence Collection
Data Capture
Analysis

Next Step
Identify the system(s) that have been affected
Identify user credentials compromised or at risk
Identify the IT services being impacted
Identify additional system(s) that are at risk of being compromised
Identify malicious code on any systems linked to fraudulent sites
Identify business implications of the attack
Identify any source attribution collected
Identify how widespread the attack has spread
Identify the tools used to detect the attack

Servers  | Desktop  | Laptop  | Mobile  | VM  | LDAP Directory
---|---|---|---|---|---
Incident Database  | Threat Database |
Select Database  | Vulnerability Logs  | System Logs  | Query Database  | Generate Report
View Report  | View Record Details  | Select Records  | Copy Record Details  |
SIEM  | IDS  | Firewall  | Scanners  | Antivirus  | Spam Filter
Eradicate Malware

- Request System Patch, Rule Update, or Content Filter Modification
- Test Implementation
- Contain Phishing Sample
- Test malware eradication procedure

Communications

- Direct Phone Call
- Conference Call
- In-Person Meeting
- Intranet Meeting
- Mobile Messaging
- Internet Meeting

Triage & Confirm Incident Report

- Add/Change/Remove Affected System/Site/Network
- Coordinate Technical Counter-Measures & URL Redirect With ISP
- Coordinate With 3rd Party Take Down Service

Prev Step

Next Step
Incident Review

Lessons Uncovered

Lessons Applied

Response Workflow Updated

Electronic Personal Health Information (ePHI) Compromised?

Sensitive Government Information Compromised?

Discovery Meeting

Policy Updates Defined

Process Updates Defined

Configuration Updates Defined

Policies Implemented

Process Changes Implemented

Configurations Applied

END
Proactive Response
An automated playbook helps security teams optimize for efficiency and productivity. Your security team has the ability to analyze, detect and prioritize when all pertinent data and multiple security tools are integrated into one system. With one-screen visibility you can identify anomalies, assign tasks, access reporting and communicate across multiple departments effectively for quick responses.

Quick Containment
Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organization and taking the proper steps mitigate damage.

Effective Remediation
Organization and automation are key benefits that result in effective remediation. Automated playbooks help to organize security processes, mitigation plans and smooth communication between multiple departments. By optimizing data collection, analysis, and communications you improve the odds for effective eradication, recovery with integrity and forensic-quality reporting.

Security Management Benefits
- Be prepared to handle any incident your team faces
- Control the situation, minimizing the impact to the business
- Efficiently manage your response across multiple departments

Useful Links:
- NIST Incident Handling Guide
- SANS Incident Handler’s Handbook

Risk Management Benefits
- Communicate effectively to ensure risk mitigation methods are applied
- Prioritize resources and activities where they matter most
- Report and tune based on response learning, reducing risk moving forward

Useful Links:
- NIST Risk Management Framework Guide
- Sample Policies and Plans

Action Plan
Having a view into what is possible is the first step in taking action. The next step is to bring your team together to drive it toward reality. Email this guide to your peers and managers to begin sharing your playbook with them.

With this playbook, you will be better prepared to handle the response. To help with the management and automation of this incident response playbook, consider working with CyberSponse and their partners. Come take a look at what they do.

For additional incident response playbook examples, visit https://www.incidentresponse.com/playbooks