SCOTT MACLEAN

NOVEMBER 2024

# WORKFLOW FOR COMMON INCIDENCES PHISHING

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

To effectively mitigate the risks associated with phishing attacks, our organization has implemented a comprehensive incident response plan. This plan focuses on four key stages: Preparation, Detection and Analysis, Containment, Eradication, and Recovery, and Post-Incident Activity.

During the Preparation phase, we identify key roles, develop incident response procedures, implement technical controls, and conduct regular testing and drills. Detection and Analysis involves continuous monitoring of systems, identifying suspicious activity, analyzing incidents, and collecting evidence. In the Containment, Eradication, and Recovery phase, we isolate affected systems, remove malware, patch vulnerabilities, recover data, and restore systems. The Post-Incident Activity phase focuses on conducting a thorough review, implementing corrective actions, updating security policies, and providing ongoing employee training.

To detect potential phishing attacks, we monitor for various triggers and indicators of compromise (IoCs). These include unusual email senders, urgent tone, suspicious links and attachments, poor grammar, generic greetings, requests for sensitive information, malicious URLs, malicious attachments, unusual network traffic, abnormal login activity, compromised accounts, data exfiltration, and system anomalies.

By proactively implementing this incident response plan and staying vigilant for potential phishing attacks, we aim to significantly reduce the risk of successful attacks and protect our organization's valuable assets.

# STEP ONE - PREPARATION

1. Identify Key Roles and Responsibilities
   - Team Leader: Misha - Regular, Minka - Afterhours: Oversees the incident response process.
   - IT Specialist: Ned analyzes security threats and vulnerabilities.
   - Network Administrator: Lucky manages network infrastructure and security.
   - Data Administrator: Dusty manages system and data security.
   - MSPP Specialist - Cat is the external consultant for MSPP
2. Implement Controls
   - Email Security: Deploy email security solutions, such as spam filters, antivirus software, and email authentication protocols.
   - Web Filtering: Implement web filtering to block access to malicious websites.
   - User Awareness Training: Conduct regular security awareness training to educate employees about phishing tactics and best practices.
3. Develop Communication Plan [1]
   - Internal Communication: Establish communication channels for informing employees about the incident and providing updates.
   - External Communication: Have emails and phone numbers ready for when you need to escalate issues.
4. Conduct Regular Testing and Drills
   - Tabletop Exercises: Conduct simulated phishing attacks to test the incident response team's readiness.
   - Technical Testing: Regularly test security controls and incident response tools.

# STEP TWO - DETECTION

1.Continuous Monitoring and Logging

- Email Logs: Data must monitor email logs for unusual activity, such as mass email campaigns, suspicious attachments, or links.
- Web Logs: Network Specialists must monitor web logs for unusual traffic patterns or attempts to access unauthorized resources through scans.
- Security Event Logs: IT must monitor security event logs for alerts related to phishing attacks, such as failed login attempts or malicious code execution.

2. Incident Detection and Alerting

- Email Security Systems: Configure email security systems to detect and block phishing emails.
- User Reporting: Encourage employees to report suspicious emails to the security team.
- Security Information and Event Management (SIEM): Use SIEM to correlate security events and identify potential phishing attacks.

## TRIGGER

3. Event

- If there is an indication that there has been a phishing email sent out, immediately send company wide notification warning to all employees about email and external notification to Cat.
- Infection Analysis: Identify compromised systems and the extent of the breach.
- Data Exfiltration Analysis: Data specialist will determine if sensitive data has been compromised or permissions changed.
- IT will determine if any sensor thresholds, such as bandwidth, are being exceeded
- Network will scan packets using Wireshark to determine any suspicious requests.

# STEP TWO - DETECTION

## CONTINUED

4. Evidence Collection and Preservation
   - Preserve Evidence: Preserve link for future forensics
5. Threat Intelligence Gathering
   - Analyze any other Indicators of Compromise (IOCs): IT, network and data will scan for any other IOC’s to try and track down what is causing this.

# STEP THREE - CONTAINMENT, ERADICATION AND RECOVERY

If it has been deemed that an employee has clicked a malicious link, downloaded any software or that any malicious actors are in the system, immediately escalate the case to the team lead and send out notifications to the IT, Network and Data departments. Inform Cat of escalation and IoC's used to determine this. Lastly send notification to CEO. After notifications have been sent, Cat and her team will advise on the steps outlined.

1. Containment
   - Isolate Affected Systems: Disconnect compromised systems from the network to prevent further spread of the attack.
   - Restrict Network Access: Block all suspicious URL's found on the alerts and block IP addresses with firewall
   - Disable Compromised Accounts: Disable user accounts that may have been compromised.
2. Eradication
   - Remove Malicious Software: Scan affected systems for malware and remove any malicious files.
   - Patch Vulnerabilities: Apply security patches to address vulnerabilities exploited in the attack.
   - Reset Compromised Passwords: Reset passwords for compromised accounts.
3. Recovery [1]
   - Data Recovery: Recover any lost or corrupted data from backups.
   - System Restoration: Restore affected systems to a clean state.
   - Network Restoration: Restore network connectivity and security configurations.

# STEP FOUR - POST-INCIDENT ACTIVITY

1. Post-Incident Review [1]
   - Document the Incident: Create a detailed incident report, including timelines, actions taken, and outcomes.
   - Evaluate Incident Response Effectiveness: Assess the effectiveness of the incident response team and procedures.
2. Improvement
   - Enhance Security Controls: Strengthen security controls, such as email filtering, web filtering, and user awareness training.
3. Communication and Reporting
   - Internal Communication: Communicate the incident and its resolution to employees.
   - External Communication: Communicate with affected parties, such as customers if necessary.
   - Regulatory Reporting: Report the incident to relevant regulatory authorities, if required.
4. Continuous Improvement
   - Regular Security Audits: Conduct regular security audits to identify and address potential vulnerabilities.
   - Employee Training: Provide ongoing security awareness training to employees.
   - Stay Informed on Emerging Threats: Stay updated on the latest phishing techniques and threats.

# POSSIBLE TRIGGERS AND IOC'S

Triggers:

- Unusual Email Sender: Emails from unexpected senders, especially those impersonating legitimate organizations.
- Urgent Tone and Sense of Urgency: Emails that demand immediate action, often using fear or threats.
- Suspicious Links and Attachments: Emails containing links to unfamiliar websites or attachments with unexpected file extensions.
- Poor Grammar and Spelling: Phishing emails often have grammatical errors or typos.
- Generic Greetings: Emails that use generic greetings like "Dear User" or "Dear Customer."
- Requests for Sensitive Information: Emails asking for personal information, such as passwords, credit card numbers, or social security numbers.

Indicators of Compromise (IoCs):

- Unusual Network Traffic: Increased network traffic to suspicious IP addresses or domains.
- Abnormal Login Activity: Unusual login attempts from unfamiliar locations or devices.
- Compromised Accounts: Unauthorized access to user accounts.
- Data Exfiltration: Unusual data transfer activity, such as large file downloads or data uploads to external servers.
- System Anomalies: Unexpected system behavior, such as slow performance, frequent crashes, or unusual error messages.

# CITATIONS AND REFERENCES

1. Cybersecurity Incident & Vulnerability response playbooks. (n.d.). https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

2. The SOC methodology. SecureGlobal. (2018, June 19). https://secureglobal.de/the-soc-methodology

3. What is a workflow? A beginner's Guide to Workflow Management: Process street: Process & project management software. Process Street | Process & Project Management Software | The collaboration platform for teams that care about quality & compliance. (2024, March 5). https://www.process.st/what-is-a-workflow/

# LETTER TO CLIENT

Dear Percy,
We are writing to inform you of a recent cyber security incident that affected our systems. We understand that this incident may have caused concern, and we want to assure you that we took immediate action to mitigate the impact.

Upon detection of the incident, our security team promptly initiated a comprehensive response plan. This involved:

- Incident Response: Our security experts worked diligently to contain the threat and prevent further damage.
- Investigation: A thorough investigation was conducted to determine the root cause and scope of the breach.
- Remediation: Necessary steps were taken to restore compromised systems and implement additional security measures.

We are pleased to inform you that the incident has been successfully addressed, and our systems are now fully operational.
To further enhance our security posture and prevent future incidents, we are implementing additional security controls, including:

- Employee Awareness Training: We will be conducting regular training sessions to educate our employees about the latest cyber threats and best practices for protecting sensitive information.
- Enhanced Security Monitoring: Our security team will continue to monitor our systems closely for any signs of suspicious activity.

We take the security of your data very seriously, and we are committed to maintaining the highest standards of information security. If you have any questions or concerns, please do not hesitate to contact us.
Thank you for your understanding and continued trust.

Sincerely,
Scott Maclean

# LETTER TO 3RD PARTY PROVIDER

Dear Cat,

We are writing to provide a formal notification regarding a recent cyber security incident that occurred on recently.

Incident Summary:
Phishing and attempted DDoS attack.

Incident Response Actions:
Upon detection of the incident, our security team, in collaboration with your team, initiated the following response actions:

- Containment: Disconnected the effected employee computer.
- Investigation: After receiving a report of a suspicious email, we used a VM not connected to our network to go to the suspicious URL. After clicking the link we analyzed data packets from Wireshark to see a large number of ping requests.
- Remediation: After disconnecting the effected computer from the network, we made sure to send an organizational wide email to say not to click the link and then updated our firewall settings to block IP's.

Lessons Learned and Future Mitigation:

To prevent similar incidents in the future, we have identified the following key lessons:

- We need to increase employee awareness by introducing training protocols
- We need to introduce more monitoring controls to scan for these malicious emails

Based on these insights, we will implement the following mitigation strategies:

- Network segmentation - separating the employee computers onto VLAN's
- Enhanced employee awareness training

We appreciate your prompt response and support throughout this incident. Your expertise and collaboration were instrumental in minimizing the impact and ensuring a swift recovery. Please let us know if you require any further information or have any questions.

Sincerely,
Scott Maclean