Seneca

Deliverable 2: Incident Response Plan

SEC715NAA.07597.2244

Security Management

Submitted By:

Bhupendra Mouny

Arman Lamba

Sarthak Nilesh Shah

Gaganjot Singh

(GROUP 4)

Submitted To:

Amir Ramezanpour

2nd August 2024

Table of Contents

Executive summary:

This incident response plan outlines our financial institution's strategy for managing cybersecurity incidents, with the primary objectives of protecting critical assets, maintaining customer trust, and ensuring business continuity. It features a dedicated incident response team with clearly defined roles, following NIST 800-61r2 guidelines. Our approach includes a four-phase process: Preparation involves developing necessary policies, procedures, and technical capabilities; Detection and Analysis focuses on identifying and assessing breaches through continuous monitoring; Containment, Eradication, and Recovery aim to swiftly isolate affected systems, eliminate threats, and restore normal operations; and Post-Incident Activity centers on reviewing and enhancing our response capabilities and overall security posture.

Additionally, the plan includes detailed checklists and procedures tailored to our specific needs and regulatory requirements. A robust communication strategy ensures timely information sharing with stakeholders, customers, regulators, and law enforcement. Regular testing and updates are integral to maintaining the plan's effectiveness against emerging threats. Overall, this plan is designed to minimize the impact of security incidents, safeguard customer information, and ensure compliance with industry regulations, reflecting our commitment to proactive and effective cybersecurity practices.

Phishing Incident Response Plan for Financial Institutions

Executive Summary of phishing Incident

This IRP will help our financial institution to manage and mitigate the phishing incident effectively. Since we deal with sensitive data like names, addresses, Social Insurance Numbers, bank account numbers, and financial transaction information, rigorous response against phishing threats is of prime importance. The plan points out the measures to be taken regarding preparation, detection, analysis, containment, eradication, recovery, and lessons learned from the incident regarding phishing incidents, ensuring the security and integrity of our clients' private information.

It follows most of the guidelines outlined in NIST Special Publication 800-61r2, laying great emphasis on a structured approach in incident handling. These critical phases include preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. Our institution is going to apply this plan for reducing the damage caused by phishing attacks, to safeguard the trust of the clients, and to act according to all applicable regulatory requirements.

Team Members, Roles, and Responsibilities

The Incident Response Team (IRT) comprises key personnel responsible for managing and mitigating phishing incidents effectively.

- **Incident Response Coordinator**

  The Incident Response Coordinator takes the leading roles throughout the incident response process. Their main role is to oversee the coordination of the response

efforts, communication between stakeholders, and overall adherence to the Incident Response Plan.

- **Security Analysts**

  Detection, analysis, and investigation of the phishing incident are all within the hands of Security Analysts. They monitor systems for phishing attempts and give technical expertise toward addressing and mitigating threats.

- **IT Support Staff**

  IT Support Staff provide technical support during incident response. They implement technical controls, aid in threat containment and eradication, and restorers of systems to normal state operations.

- **Legal Counsel**

  It ensures compliance with the related legal and regulatory requirements through Legal Counsel. It does so by advising regarding the legal implications and managing communications with regulators, and handling any legal issues which may be the result of the incident.

- **Public Relations (PR) Team**

  The PR Team is responsible for communications with third-party stakeholders. They shall prepare public statements, handle contacts with the media, and try to protect the reputation of the organization during the entire incident.

- **Human Resources (HR)**

  HR looks after internal personnel matters regarding the incident. They are responsible for internal communication, assistance to the affected employees, and any kind of disciplinary action needed to keep order and morale within the organization.

Incident Response Checklist

Preparation

- Ensure all staff are trained on recognizing phishing attempts.
- Maintain updated incident response playbooks.
- Conduct regular phishing simulations.
- Ensure all systems are updated and patched.
- Have incident response tools and technologies in place.

Detection and Analysis

- Monitor email systems and user reports for phishing attempts.
- Analyze phishing emails to determine scope and potential impact.
- Document and escalate the incident as needed.

Containment, Eradication, and Recovery

- Isolate affected systems to prevent further spread.
- Remove phishing emails from all user inboxes.
- Conduct a thorough investigation to remove malicious content.
- Restore affected systems from backups.
- Monitor for any signs of persistent threats.

Post-Incident Activity

- Conduct a post-mortem analysis to understand the incident's root cause.
- Update incident response plans and training based on lessons learned.
- Report the incident to relevant regulatory bodies if required.
- Communicate with affected clients and provide support.

Preparation

In the preparation phase, our financial institution works to establish a solid defense against phishing attacks. Several principal activities are required:

1. **Training and Awareness:** Our institution trains all employees regularly to allow them to be better armed against identifying and reporting a phishing attempt. This includes phishing simulation exercises to test and improve reactions.
2. **Policy and Procedure Development:** Proper policies and procedures are developed and communicated so that roles and responsibilities in case of any phishing attack are very clear.
3. **Technology and Tools:** State-of-the-art email filtering solutions, anti-phishing software, and other security tools implemented to detect and block phishing attempts. Keeping all systems up to date by applying updates and patches for countering vulnerabilities.
4. **Incident Response Playbooks:** Detailed playbooks for the response to phishing incidents are designed and refreshed periodically. These playbooks include step-by-step instructions to ensure an effective response to an incident.

5. **Communication Plans:** Clear channels of communication and protocols concerning internal and external communication during an event are established.

Detection and Analysis

The detection and analysis phase involves the processes by which organizations identify a phishing incident and comprehend its scope and impact. This phase involves the following main activities:

1. **Monitoring and Detection:** Even while email systems, network traffic, and user reports are continuously monitored, there can be possibilities of phishing. Automated systems and manual reviews are used to detect suspicious activities.
2. **Preliminary Analysis:** The security analysts will make some independent analysis on the phishing email to establish its authenticity, source, and likely effect. This involves checking the headers of the email, content, and links or attachments.
3. **Incident Documentation:** Information regarding the phishing incident shall be documented, including time of detection, users affected, and the nature of the phishing.
4. **Incident Escalation:** When the need has been found, incident information will be escalated to appropriate personnel and teams for additional investigation and response.
5. **Impact Assessment:** The extent of incident information shall be identified, such as the number of users affected, the type of information involved, and how much potential damage this would cause to the organization.

Containment, Eradication, and Recovery

In this phase, efforts are focused on containing the incident, removing the threat, and restoring normal operations. Key activities include:

1. Containment:

- The phishing attack is contained by blocking the mail, isolating systems infected, and restricting access of compromised accounts.
- Informing users whose information has been compromised and advising them about how to protect their personal information.

2. Eradication:

- Investigation of the incident to trace all instances of the phishing threat in a network and remove them.
- Removal of malicious emails, links, attachments, etc., from user inboxes.
- Password resetting of any comprised credentials, running of scans on systems to identify malware

3. Restitution

- Restore of affected systems and data from clean backups
- Monitoring of the systems for residual threat
- Conduct detailed reviews to ensure that all malicious content had been removed and that the systems are functioning normally.

Post-Incident Activity

The last mile involves incident analysis for improvement, so that it does not happen again in the future. This mainly comprises the following activities:

1. **Post-Mortem Analysis:** Reviewing the details of the incident to explain its root cause and the effectiveness of the response, and any gaps in the process.
2. **Lessons Learned:** Documenting lessons learned from the incident and updating incident response plans, playbooks, and training materials as per the same.
3. **Reporting:** It involves the writing of detailed reports for internal stakeholders and to the regulatory bodies in case of requirement. This would comprise a report on the timeline of the incident, the actions and the outcome.
4. **Client notification:** Alerting the clients whose information has been accessed or exposed about the incident, the steps taken to secure the clients' information and whether there is any step to be taken on their part, with offering assistance and support as required.
5. **Continuous Improvement:** The improvement actions to the security posture of the organization by learning from this experience. This includes updating the policies, enhancement of the training programs, and new technologies to improve the detection and prevention of phishing attacks.

By having this Incident Response Plan in place, our financial institution will be more capable and ready to face phishing incidents, perform effective incident handling, and minimize impacts to the sensitive information of our clients.

Malware Incident Response Plan for Financial Institutions

Executive Summary of Malware Incident Response

This incident response plan outlines our financial institution's comprehensive strategy for addressing malware threats. In the rapidly evolving landscape of cybersecurity, malware poses a significant risk to our operations, customer data, and financial assets. This plan is designed to provide a structured approach to detecting, containing, and eradicating malware threats while ensuring business continuity and regulatory compliance.

Our plan is tailored to address various types of malware threats, including but not limited to ransomware, trojans, keyloggers, rootkits, worms, and spyware. By implementing this plan, we aim to protect the integrity of our financial systems and customer data, maintain customer trust and confidence in our institution, ensure compliance with financial sector regulations and data protection laws, and minimize financial losses and reputational damage from malware incidents.

Key components of our plan include:

- A dedicated Incident Response Team with clearly defined roles and responsibilities.
- Comprehensive preparation measures.
- Advanced detection and analysis protocols.
- Robust containment and eradication procedures.
- Thorough post-incident review and improvement processes.

This plan will be regularly reviewed and updated to address emerging threats and incorporate lessons learned from incidents and simulations.

How/When to Use

The incident response plan is an essential part of an organization's security infrastructure, designed to be activated in response to suspicious activities or events. Its main goal is to quickly neutralize threats to minimize damage and reduce the financial impact on the organization.

Key response measures include:

- Identification
- Containment
- Eradication & Recovery
- Post-Incident Activities

Team Members, Roles, and Responsibilities

Our Incident Response Team consists of the following roles, aligned with NIST 800-61r2 guidelines:

Incident Response Manager

- Oversees the entire response process from detection to post-incident review.
- Coordinates with senior management, the board of directors, and external stakeholders.

- Makes critical decisions on resource allocation, incident classification, and escalation.
- Ensures compliance with regulatory reporting requirements.
- Authorizes major containment and eradication actions.

Security Analyst

- Leads the technical investigation of malware incidents.
- Analyzes system logs, network traffic, and malware samples.
- Recommends and implements containment strategies.
- Coordinates with threat intelligence services to identify malware strains and attack vectors.
- Performs regular security assessments and vulnerability scans.

Network Administrator

The Network Administrator monitors network traffic for signs of malware activity and implements network-level containment measures. They assist in restoring secure network operations post-incident, manage and update network security appliances, and conduct regular network security audits.

System Administrator

The System Administrator manages affected systems and applications, implementing system-level containment and eradication measures. They assist in system recovery and hardening, maintain and update system backups, and manage patch management and system updates.

Communications Coordinator

- Manages internal communications to keep staff informed.
- Prepares external communications for customers, partners, and media.
- Ensures compliance with regulatory reporting requirements.
- Coordinates with the PR team for public-facing communications.
- Maintains a log of all communications during the incident.

Legal Advisor

- Provides guidance on legal and compliance issues.
- Assists in determining regulatory notification requirements.
- Advises on potential legal implications of response actions.
- Liaises with law enforcement agencies if necessary.
- Reviews all external communications before release.

Forensic Specialist

The Forensic Specialist conducts in-depth analysis of malware samples, preserves evidence for potential legal proceedings, and assists in determining the scope and impact of the malware incident. They perform data recovery from affected systems when necessary and provide technical input for incident reports and regulatory filings.

Incident Response Checklist

Preparation

- **Training:** Regular security training.
- **Antivirus:** Maintain updated antivirus solutions.
- **Backups:** Establish and test secure backups.
- **Inventory:** Keep an updated asset inventory.
- **Access Controls:** Implement strict access controls and multi-factor authentication.
- **Assessments:** Conduct regular vulnerability assessments.
- **Relationships:** Establish connections with law enforcement and threat intelligence providers.
- **Playbooks:** Maintain incident response playbooks.
- **Segmentation:** Isolate critical systems.
- **Testing:** Regularly test and update the response plan.

Detection and Analysis

- **Monitoring:** 24/7 system and network monitoring.
- **Alert Analysis:** Analyze security alerts.
- **Investigate:** Investigate unusual activities.
- **Assessment:** Assess impact on operations and data.
- **Classification:** Classify incidents by severity.
- **Identification:** Identify malware type.
- **Infection Vector:** Determine infection source and spread.

- **Data Exfiltration:** Assess potential data exfiltration.
- **Documentation:** Document findings and report.

Containment, Eradication, and Recovery

Containment

- **Isolation:** Isolate affected systems.
- **Disable Access:** Disable compromised accounts.
- **Monitoring:** Enhance monitoring and controls.
- **Block:** Block malware communication channels.
- **Evidence:** Preserve forensic evidence.

Eradication

- **Removal:** Remove malware using approved tools.
- **Patch:** Patch vulnerabilities.
- **Update Controls:** Strengthen security controls.
- **Verify:** Ensure integrity of applications and data.

Recovery

- **Restore:** Use clean backups to restore systems.
- **Security:** Implement enhanced security controls.
- **Testing:** Test restored systems thoroughly.
- **Monitoring:** Monitor systems closely post-recovery.

Post-Incident Activity

- **Review:** Conduct a thorough review of the incident.
- **Report:** Provide detailed reports to management and regulatory bodies.
- **Training:** Update staff training based on insights.
- **Policies:** Revise security policies and controls.
- **Assessment:** Conduct follow-up security assessments.
- **Sharing:** Share incident information with industry peers.

Preparation

Preparation is crucial for effective malware incident response. Our financial institution conducts regular security awareness training for all employees, focusing on malware prevention and safe computing practices. We implement and maintain up-to-date antivirus and anti-malware solutions across all systems, ensuring regular updates and scans. Secure backup systems for critical financial data and applications are established and tested regularly, with offline copies maintained.

- Develop and update an asset inventory of all systems, applications, and data, prioritizing critical assets.
- Implement strict access controls, multi-factor authentication, and least privilege principles across all systems.
- Conduct regular vulnerability assessments and penetration testing to identify and address potential weaknesses.

- Establish relationships with law enforcement, financial sector CERT, and threat intelligence providers for timely information sharing.
- Develop and maintain incident response playbooks for different types of malware, including specific procedures for financial systems.
- Implement network segmentation to isolate critical financial systems from potentially compromised areas.
- Regularly test and update the incident response plan through tabletop exercises and simulations, involving all team members and relevant stakeholders.

Detection and Analysis

Effective detection and analysis are key to mitigating the impact of malware incidents. Our approach includes 24/7 monitoring of all systems and networks for signs of malware activity using SIEM, EDR, and other security tools. Alerts from SIEM, IDS/IPS, antivirus, and anomaly detection systems are analyzed, with a focus on financial transaction anomalies.

- Investigate unusual account activity, unauthorized access attempts, or unexpected system behavior, particularly in core banking systems.
- Conduct initial assessment of potential malware impact on financial operations and customer data, prioritizing critical systems.
- Determine if customer data or financial assets are compromised or encrypted, initiating customer protection measures if necessary.
- Classify the incident based on severity, potential financial impact, and regulatory implications, with high-priority incidents escalated immediately.

- Identify the type and strain of malware involved using threat intelligence and malware analysis tools.
- Determine the initial infection vector and potential spread within the network, focusing on the impact on interconnected financial systems.
- Assess the potential for data exfiltration or financial fraud resulting from the malware, initiating fraud prevention measures if needed.
- Document all findings and create an initial incident report for the Incident Response Manager and relevant stakeholders.

Containment, Eradication, and Recovery

This phase focuses on limiting the damage, removing the threat, and restoring normal operations.

Containment

- Isolate affected systems and segments of the network to prevent malware spread, prioritizing the protection of core financial systems.
- Disable network access for compromised accounts and systems, especially those with access to sensitive financial data or transaction capabilities.
- Implement additional monitoring and access controls on critical financial systems to detect any ongoing malicious activity.
- Block communication to known malware command and control servers, updating firewall rules and intrusion prevention systems.

- Preserve forensic evidence for later analysis and potential legal proceedings, ensuring chain of custody for all collected data.

Eradication

Malware is removed using approved tools and procedures, ensuring thorough cleaning of all affected systems. Vulnerabilities exploited for initial infection are patched, prioritizing critical security updates. Security controls are updated and strengthened to prevent similar infections, including enhancing endpoint protection and access controls. Thorough scans of all systems are conducted to ensure complete malware removal, with special attention to financial processing systems. The integrity of critical financial applications and databases is verified to ensure no unauthorized changes or data corruption.

Recovery

- Restore systems using clean, verified backups, prioritizing core financial services to minimize downtime.
- Implement additional security controls based on lessons learned, such as enhanced monitoring or stricter access policies.
- Verify integrity of financial data and transactions, reconciling accounts and transactions as necessary.
- Gradually restore services, prioritizing critical financial operations and customer-facing systems.
- Conduct thorough testing of restored systems before returning them to production, including security and functionality tests.

- Monitor recovered systems closely for any signs of persistent malware or abnormal activity, maintaining heightened vigilance for an extended period.

Post-Incident Activity

After the incident is resolved, we focus on learning and improvement. A thorough review of the incident response process and its effectiveness is conducted, involving all team members and relevant stakeholders. The financial and operational impact of the incident is assessed, including direct costs, lost business, and potential long-term effects on customer trust. Areas for improvement in detection, containment, and eradication procedures are identified, and the incident response plan is updated accordingly.

- Update incident response procedures and playbooks based on lessons learned, incorporating new insights into malware behavior and effective countermeasures.
- Provide detailed reports to senior management, the board of directors, and relevant regulatory bodies, ensuring full transparency and compliance.
- Conduct additional staff training based on incident insights, reinforcing security awareness and incident response procedures.
- Review and update security policies, controls, and technologies, addressing any gaps identified during the incident.
- Assess potential long-term impacts on customer trust and financial operations, developing strategies to mitigate any reputational damage.
- Conduct a follow-up security assessment to verify the effectiveness of new controls and identify any remaining vulnerabilities.

- Share sanitized incident information with industry peers and relevant ISACs to improve sector-wide resilience against similar malware threats.

By following this comprehensive incident response plan, our financial institution can effectively manage and mitigate the impact of malware incidents, protecting our assets, customers, and reputation while maintaining regulatory compliance and operational resilience.

Ransomware Incident Response Plan for Financial Institutions

Executive Summary

This Incident Response Plan is developed to help our financial institution in the effective management and mitigation process of ransomware incidents. We deal with a quantity of sensitive information, like names, addresses, Social Insurance Numbers, bank account numbers, and financial transaction information; hence, a robust response against ransomware attacks is called for. This strategy details out the steps that will be conducted toward the preparation, detection, analysis, containment, eradication, recovery, and lessons learned from ransomware incidents, ensuring the security and integrity of private information belonging to our clients.

The IRP takes after NIST Special Publication 800-61r2, where the approach to incident handling is structured into five key phases: preparation, detection and analysis, containment, eradication and recovery, and finally, post-incident activity. Compliance with this plan will help the organization reduce the impact of ransomware attacks on clientele, uphold the trust of the clients in the company's services, and ensure conformance with various regulations.

Team Members, Roles, and Responsibilities

The following are key personnel, which consist of the Incident Response Team for the management and mitigation of ransomware incidents.

- **Incident Response Coordinator**

The Incident Response Coordinator ensures that all processes involved in incident response are managed and coordinated. This includes response effort management, stakeholder communication, and follow-up on the Incident Response Plan.

- **Security Analysts**

  The Security Analysts detect, analyze, and investigate ransomware incidents. Among others, the duties include monitoring of systems for ransomware threats, analysis, and providing technical expertise to respond to and proactively mitigate threats.

- **IT Support Staff**

  The IT Support Staff provides technical support during incident response. Their tasks include implementation of technical controls, threat containment and eradication, and system restoration to normal operational state.

- **Legal Counsel**

  The Legal Counsel ensures that the activities of the incident response team are performed in accordance with all applicable legal and regulatory requirements. The legal implications of each action are advised by them, the communication with regulators is handled, and any litigation that could arise from the incident is managed.

- **Public Relations Team**

  The PR Team manages communication with parties external to the organization. They prepare public statements, respond to media inquiries, and seek to protect the reputation of the organization during the incident.

- **Human Resources**

HR tends to internal personnel issues related to the incident and manages the internal communication and support of staff affected by what happened. They also handle any disciplinary actions to retain order and morale within the organization.

Incident Response Checklist

1. **Preparation**
    - Conduct regular training on ransomware threats and response protocols.
    - Maintain updated incident response playbooks.
    - Ensure all systems are regularly backed up and patches are up-to-date.
    - Implement strong security measures, including endpoint protection and network segmentation.
    - Have incident response tools and technologies in place.
2. **Detection and Analysis**
    - Monitor systems for signs of ransomware activity.
    - Analyze suspicious activities and determine the scope and impact of the ransomware.
    - Document and escalate the incident as needed.
3. **Containment, Eradication, and Recovery**
    - Isolate affected systems to prevent the spread of ransomware.
    - Remove ransomware and any associated malware from systems.

- Restore affected systems and data from backups.
- Monitor for any signs of persistent threats.

4. **Post-Incident Activity**
   - Conduct a post-mortem analysis to understand the incident's root cause.
   - Update incident response plans and training based on lessons learned.
   - Report the incident to relevant regulatory bodies if required.
   - Communicate with affected clients and provide support.

Preparation

In the preparation phase, our financial institution works on the establishment and maintenance of robust defenses against ransomware attacks. This includes some of the following key activities:

1. **Training and Awareness:** Routine training on ransomware attacks will be provided to all employees in order for them to be able to identify and respond properly to ransomware threats. Running simulations for a ransomware attack, testing, and improving the reaction is included.
2. **Policy and procedure development:** Develop clear policies and procedures in case of a ransomware incident and make them known to all, specifying who shall be responsible for what.
3. **Technology and tools:** Enhanced endpoint protection along with network segmentation, as well as security tools to detect and block attempts to get infected by

ransomware. Of course, all systems would have had their updates and patches in order not to fall into the trap.

4. **Incident Response Playbooks:** Detailed playbooks for ransomware incident response are designed and updated frequently for step-by-step process guides in incident handling.
5. **Data Backup and Recovery Plans:** Backups of all critical data are done frequently, and the recovery plans are tested to restore operations quickly when attacked.
6. **Communication Plans:** Internal and external communication channels and protocols for incidents are clearly defined.

Detection and Analysis

The detection and analysis phase involves identifying and understanding the scope and impact of a ransomware incident. Key activities include:

1. **Monitoring and Detection:** It views and monitors the systems, network traffic, and users' reports continuously to identify any possible ransomware activity. The detection of ransomware comes with automated systems complemented by manual reviews for suspicious behavior.
2. **Preliminary Analysis:** Security analysts conduct a preliminary or superficial analysis of the ransomware to determine its type, source, and probable impact. It is based on the encrypted files viewed, ransom notes, and any indicators of the network.
3. **Documentation of the Incident:** Document every relevant detail concerning the ransomware incident, like time of detection, affected systems, and what kind of attack it was.

4. **Incident Escalation:** The information acquired through the primary analysis is used to escalate the incident to relevant personnel and teams for further investigation and response.
5. **Impact Assessment:** It is realized through the extent of the incident, including how many systems are affected, what type of data has been targeted, and how the organization can potentially be damaged.

Containment, Eradication, and Recovery

At this stage, priorities are incident containment, threat removal, and restoration of normal operations. Activities include:

1. **Containment:**
   - Urgent measures to contain the ransomware spread, such as isolation of affected systems and networks.
   - Information to the users about the incident and the ways to protect information.
2. **Eradication:**
   - Conducting a thorough investigation to identify and remove all traces of the ransomware threat from the network
   - Ensure that all compromised credentials are reset, and systems are on watch for further malware.
3. **Recovery**
   - Restore compromised systems and data from clean backups.
   - Syslog monitoring for any residual threat in systems.

- Ensure through review that all malicious content has been cleaned and systems are running in normal condition.

Post Incident Activity

The last phase is incident analysis and making improvements to prevent such incidents in the future. Activities:

1. **Post-Mortem Analysis:** Detailed review of the incident to understand its root cause, how effective the response was, and any process gaps that may exist.
2. **Lessons Learned:** Document what was learned from the incident; update incident response plans, playbooks and trainings appropriately.
3. **Reporting:** Proper reporting to internal stakeholders and, if necessary, to any regulatory body. This shall involve adding to the report a description of the chronology of the incident, the measures taken, and the results.
4. **Communication with Clients:** All clients whose information is compromised shall be contacted with details of the incident, the measures taken to protect their information, and the action required from their end. Support and help can be offered where necessary.
5. **Continuous Improvement:** At this stage, improvements to the security posture of the organization will be implemented, according to lessons learned. This might include updating policies, increasing the level of training programs, or implementing new technologies for the detection and blocking of ransomware attacks.

By following this Incident Response Plan, our financial institution will be better prepared to handle ransomware incidents effectively, minimize their impact, and protect the sensitive information entrusted to us by our clients.

Brute force Incident Response Plan for Financial Institutions

Executive Summary

This incident response plan outlines our financial institution's comprehensive strategy for addressing brute force attacks. Brute force attacks, which involve repeated attempts to guess passwords or encryption keys, pose a significant risk to our operations, customer data, and financial assets. This plan provides a structured approach to detecting, containing, and eradicating brute force threats while ensuring business continuity and regulatory compliance.

Our plan is tailored to address various aspects of brute force attacks, including detection, containment, and recovery. By implementing this plan, we aim to protect the integrity of our financial systems and customer data, maintain customer trust, ensure compliance with financial sector regulations, and minimize financial losses and reputational damage from such incidents.

Key components of our plan include:

- A dedicated Incident Response Team with clearly defined roles and responsibilities.
- Comprehensive preparation measures.
- Advanced detection and analysis protocols.
- Robust containment and eradication procedures.
- Thorough post-incident review and improvement processes.

Team Members, Roles, and Responsibilities

Our Incident Response Team, aligned with NIST 800-61r2 guidelines, consists of the following roles:

Incident Response Manager

- Oversees the entire response process from detection to post-incident review.
- Coordinates with senior management and external stakeholders.
- Makes critical decisions on resource allocation, incident classification, and escalation.
- Ensures compliance with regulatory reporting requirements.

Security Analyst

- Leads the technical investigation of brute force incidents.
- Analyzes system logs, network traffic, and attack patterns.
- Recommends and implements containment strategies.
- Coordinates with threat intelligence services to identify attack vectors.

Network Administrator

- Monitors network traffic for signs of brute force activity.
- Implements network-level containment measures.
- Assists in restoring secure network operations post-incident.

System Administrator

- Manages affected systems and applications.
- Implements system-level containment and eradication measures.
- Assists in system recovery and hardening.

Communications Coordinator

- Manages internal and external communications.
- Ensures compliance with regulatory reporting requirements.
- Coordinates with the PR team for public-facing communications.

Legal Advisor

- Provides guidance on legal and compliance issues.
- Assists in determining regulatory notification requirements.
- Advises on potential legal implications of response actions.
- Liaises with law enforcement agencies if necessary.

Forensic Specialist

- Conducts in-depth analysis of attack patterns.
- Preserves evidence for potential legal proceedings.
- Assists in determining the scope and impact of the incident.

Incident Response Checklist

Preparation

- Security awareness training
- Robust security solutions (firewalls, IDS/IPS, endpoint protection)
- Secure, tested backups
- Updated asset inventory
- Strict access controls and multi-factor authentication
- Regular vulnerability assessments
- Incident response playbooks

Detection and Analysis

- 24/7 monitoring (SIEM, EDR, IDS/IPS)
- Analyze security alerts and logs
- Investigate unusual activities
- Assess impact on operations/data
- Classify incidents by severity
- Identify attack type and spread
- Document findings/report

Containment, Eradication, and Recovery

Containment

- Isolate affected systems
- Disable compromised accounts
- Enhance monitoring/controls

- Block malicious communications
- Preserve forensic evidence

Eradication

- Remove threats using approved tools
- Patch vulnerabilities
- Strengthen security controls
- Conduct thorough system scans

Recovery

- Restore systems from clean backups
- Implement enhanced security controls
- Test restored systems
- Monitor post-recovery

Post-Incident **Activity**

- Review incident
- Report to management/regulators
- Update staff training
- Revise security policies

- Conduct follow-up assessments
- Share information with peers

Preparation

Preparation is crucial for effective incident response. Our financial institution implements the following measures:

- Conduct regular security awareness training for all employees, focusing on identifying and preventing brute force attacks.
- Implement and maintain robust security solutions such as firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection across all systems, ensuring regular updates and scans.
- Establish secure backup systems for critical financial data and applications, testing these systems regularly, and maintaining offline copies to ensure data integrity.
- Develop and update an asset inventory of all systems, applications, and data, prioritizing critical assets and ensuring all systems are protected.
- Implement strict access controls, multi-factor authentication, and least privilege principles across all systems to minimize the risk of unauthorized access.
- Conduct regular vulnerability assessments and penetration testing to identify and address potential weaknesses.
- Develop and maintain incident response playbooks for different types of attacks, including brute force attacks, and regularly test them through tabletop exercises and simulations.

Detection and Analysis

Effective detection and analysis are key to mitigating the impact of brute force incidents. Our approach includes:

- Monitor systems and networks 24/7 for signs of brute force attacks using security tools like SIEM, EDR, and IDS/IPS.
- Analyze security alerts and logs to identify potential threats.
- Investigate unusual account activity, unauthorized access attempts, and unexpected system behavior, particularly in core banking systems.
- Conduct initial assessments to determine the potential impact on financial operations and customer data.
- Classify the incident based on severity, potential financial impact, and regulatory implications, escalating high-priority incidents immediately.
- Identify the type and strain of the attack using threat intelligence and analysis tools, determining the initial infection vector and potential spread within the network.
- Document all findings and create an initial incident report for the Incident Response Manager and relevant stakeholders.

Containment, Eradication, and Recovery

This phase focuses on limiting the damage, removing the threat, and restoring normal operations.

Containment

- Isolate affected systems and network segments to prevent the spread of the attack.
- Disable compromised accounts and systems, especially those with access to sensitive financial data or transaction capabilities.
- Implement additional monitoring and access controls on critical financial systems to detect any ongoing malicious activity.
- Block communication to known malicious servers, updating firewall rules and intrusion prevention systems.
- Preserve forensic evidence for later analysis and potential legal proceedings, ensuring the chain of custody for all collected data.

Eradication The threat is removed using approved tools and procedures, ensuring thorough cleaning of all affected systems. Vulnerabilities exploited for the attack are patched, prioritizing critical security updates. Security controls are updated and strengthened to prevent similar infections, including enhancing endpoint protection and access controls. Thorough scans of all systems are conducted to ensure complete removal of the threat.

Recovery

- Restore systems using clean, verified backups, prioritizing core financial services to minimize downtime.
- Implement additional security controls based on lessons learned, such as enhanced monitoring or stricter access policies.
- Verify the integrity of financial data and transactions, reconciling accounts and transactions as necessary.

- Gradually restore services, prioritizing critical financial operations and customer-facing systems.
- Conduct thorough testing of restored systems before returning them to production, including security and functionality tests.
- Monitor recovered systems closely for any signs of persistent threats, maintaining heightened vigilance for an extended period.

Post-Incident Activity

After the incident is resolved, we focus on learning and improvement. A thorough review of the incident response process and its effectiveness is conducted, involving all team members and relevant stakeholders. The financial and operational impact of the incident is assessed, including direct costs, lost business, and potential long-term effects on customer trust.

- Update incident response procedures and playbooks based on lessons learned, incorporating new insights into attack behavior and effective countermeasures.
- Provide detailed reports to senior management, the board of directors, and relevant regulatory bodies, ensuring full transparency and compliance.
- Conduct additional staff training based on incident insights, reinforcing security awareness and incident response procedures.
- Review and update security policies, controls, and technologies, addressing any gaps identified during the incident.
- Conduct a follow-up security assessment to verify the effectiveness of new controls and identify any remaining vulnerabilities.

- Share sanitized incident information with industry peers and relevant ISACs to improve sector-wide resilience against similar threats.

By following this comprehensive incident response plan, our financial institution can effectively manage and mitigate the impact of brute force attacks, protecting our assets, customers, and reputation while maintaining regulatory compliance and operational resilience.

Web Application Breach Incident Response Plan for Financial Institutions

Executive Summary of Web Application Breach Incident

In today's digital landscape, protecting sensitive financial data and ensuring the security of our web applications are critical priorities. This Incident Response (IR) Plan provides a structured approach for managing and mitigating security incidents, particularly those involving breaches of our web applications. It is designed to minimize the potential impact on our financial systems, customer data, and overall organizational reputation.

The IR Plan focuses on ensuring a swift, effective, and coordinated response to security incidents. It outlines the necessary actions and responsibilities to detect, contain, eradicate, and recover from incidents, while also emphasizing the importance of post-incident activities that aim to enhance our security posture.

At the heart of this plan is our Incident Response Team (IRT), composed of professionals with specialized expertise tailored to the needs of a financial institution. The team includes roles such as an Incident Response Coordinator, Financial Security Analyst, IT Support and Infrastructure Specialist, Compliance and Legal Advisor, Risk Management Officer, and HR Representative. Each member of the team plays a crucial role in ensuring that all aspects of incident response, from technical remediation to legal compliance and communication, are comprehensively addressed.

Team Members, Roles, and Responsibilities

The Incident Response Team (IRT) plays a critical role in managing and mitigating security breaches, particularly those involving sensitive financial data and transactions. The team is composed of professionals with specialized expertise to ensure a comprehensive and effective response. Key roles within the team include:

- **Incident Response Coordinator**: Manages the entire incident response process, ensuring that all actions align with the incident response plan and comply with industry regulations. They are responsible for coordinating communication among team members and stakeholders, including regulators and auditors, and for maintaining detailed documentation of the incident and response efforts.
- **Financial Security Analyst**: A specialist focused on the security of financial systems and data. They lead the technical investigation of the breach, identifying how financial data or transactions were compromised. They implement containment, eradication, and recovery measures specific to financial systems and work closely with IT to restore secure operations.
- **IT Support and Infrastructure Specialist**: Supports the Financial Security Analyst by providing the necessary technical resources and expertise. They assist in implementing security controls specific to financial systems, monitor the performance of these systems, and ensure that all technical aspects of the response are managed effectively.
- **Compliance and Legal Advisor**: Ensures the incident response process complies with relevant financial regulations and laws, such as those set by the Financial

Conduct Authority (FCA) or similar bodies. They provide legal guidance on regulatory reporting requirements, potential liabilities, and interactions with law enforcement. They also review documentation to ensure it meets the legal standards required for audits and regulatory scrutiny.

- **Risk Management Officer**: Provides oversight from a risk management perspective, ensuring that the response aligns with the institution's risk management framework. They evaluate the potential impact of the breach on the organization's financial standing, reputation, and compliance status, and assist in making strategic decisions regarding public relations and communication with stakeholders.
- **Human Resources (HR) Representative**: Handles personnel-related issues, especially in cases where insider threats are suspected. They manage employee communications, ensure that staff are adequately informed and supported throughout the response process, and address any potential insider-related security concerns.

Incident Response Checklist

1. Preparation

- Develop and maintain the incident response plan and policies.
- Establish the Incident Response Team (IRT) with clear roles.
- Conduct regular training and deploy monitoring tools (IDS, SIEM).
- Set up communication protocols for incident reporting.

2. Detection and Analysis

- Continuously monitor systems for anomalies.

- Classify and document incidents as they are detected.
- Notify the IRT and begin analysis to determine the incident's scope.
- Identify affected assets and escalate if needed.

3. Containment, Eradication, and Recovery

Containment

- Isolate affected systems to prevent spread.
- Apply temporary fixes and monitor for new activity.

Eradication

- Remove malicious artifacts and patch vulnerabilities.
- Conduct root cause analysis.

Recovery

- Restore systems from clean backups and validate functionality.
- Gradually return systems to normal operation with ongoing monitoring.

4. Post-Incident Activities

- Conduct a post-incident review and document lessons learned.
- Update the incident response plan and security policies as needed.
- Report the incident to management, legal, and regulatory bodies if required.

5. Communication and Compliance

- Coordinate internal and external communication, including with regulators.
- Ensure compliance with reporting requirements and maintain records for audits.

Preparation

Effective incident handling begins with thorough preparation, which includes several key pre-incident activities:

- **Training and Awareness**: Regular training sessions and awareness programs ensure that all employees understand their roles in incident response and can recognize potential security incidents.
- **Implementing Security Measures**: Robust security measures, such as firewalls, intrusion detection systems (IDS), and regular patch management, are essential for preventing incidents and mitigating their impact.
- **Developing Communication Channels**: Establishing clear communication channels is critical for reporting incidents and coordinating response activities. This includes internal communication among the Incident Response Team (IRT) and external communication with stakeholders and law enforcement when necessary.

Detection and Analysis

This phase involves detecting potential incidents through monitoring tools, user reports, and system alerts. Key steps include:

- Event Detection: Utilize IDS, Security Information and Event Management (SIEM) systems, and other monitoring tools to identify anomalies.
- Initial Analysis: Analyze logs, alerts, and reports to confirm the nature and scope of the incident.

- Classification: Classify the incident based on its severity, type, and potential impact on the organization.

Containment

Containment aims to limit the damage caused by the incident and prevent further escalation. Immediate actions include:

- Short-Term Containment: Isolate affected systems, block malicious IP addresses, and disable compromised accounts.
- Long-Term Containment: Apply patches, enhance security configurations, and monitor systems for any signs of residual malicious activity.

Eradication

The eradication phase focuses on eliminating the root cause of the incident. Actions include:

- Root Cause Analysis: Investigate the source of the breach, such as identifying vulnerabilities or malware.
- Removal: Eliminate malicious code, clean affected systems, and fix vulnerabilities.
- System Hardening: Apply security patches, update software, and implement additional security controls to strengthen the system against future incidents.

Recovery

Recovery involves restoring normal operations while ensuring that the systems are secure. Key steps include:

- System Restoration: Rebuild systems from clean backups, reinstall software, and restore data to ensure a fresh start.
- Validation: Conduct thorough testing to ensure that the systems are free from malware and vulnerabilities.
- Monitoring: Intensively monitor systems post-recovery to detect any signs of persistent threats or residual issues.

Post-Incident Activities

Once an incident has been resolved and normal operations have resumed, it is essential to carry out several critical post-incident activities. These actions help the organization fully recover, learn from the event, and improve its security posture. The key post-incident activities include:

1. Documentation and Reporting

Detailed documentation of the incident and the response activities is crucial. This documentation should include:

- Incident Summary: An overview of the incident, including the type, cause, timeline, and scope.
- Response Actions: A record of all actions taken during the response, from identification and containment to eradication and recovery.
- Impact Analysis: An assessment of the incident's impact on the organization's systems, data, and operations.

- Lessons Learned: Insights into what went well and what could be improved in the response process.

This information should be compiled into a comprehensive incident report, which is shared with relevant stakeholders, including management, IT staff, and legal advisors.

2. Post-Incident Review

Conducting a thorough post-incident review, often referred to as a "lessons learned" session, is essential for continuous improvement. The review process includes:

- Review Meeting: Organizing a meeting with the incident response team and other involved parties to discuss the incident and response efforts.
- Root Cause Analysis: Performing a detailed analysis to identify the root cause of the incident and any contributing factors.
- Response Evaluation: Evaluating the effectiveness of the response, including the speed and coordination

References:

Cichonski, Paul, et al. "Computer Security Incident Handling Guide." National Institute of Standards and Technology, Aug. 2012, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
"Incident Response Plan." Cybersecurity and Infrastructure Security Agency, www.cisa.gov/incident-response-plan. Accessed 31 July. 2024.

Kral, Patrick. "Incident Handler's Handbook." SANS Institute, 5 Feb. 2012, www.sans.org/white-papers/33901/.
"Malware." Cybersecurity and Infrastructure Security Agency, www.cisa.gov/topics/malware. Accessed 1 Aug. 2024.

"Security Tip (ST04-015): Understanding and Defending Against Password-Based Attacks." Cybersecurity and Infrastructure Security Agency, www.cisa.gov/news-events/news/understanding-and-defending-against-password-based-attacks. Accessed 2 Aug. 2024.

National Institute of Standards and Technology. (2012). Computer security incident handling guide *(Special Publication 800-61 Revision 2). U.S. Department of Commerce.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Kissel, R., Scholl, M., Skolochenko, S., & Li, X. (2016). Guide for cybersecurity event recovery (NIST Special Publication 800-184). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

CERT Coordination Center. (2021). Ransomware incident response. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/stopransomware/ransomware-guide

SANS Institute. (2004). Incident handler's handbook. SANS Reading Room. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Microsoft. (2020). Protect your organization from ransomware. Microsoft Documentation. https://docs.microsoft.com/en-us/security/compass/ransomware-response