**IR Plan, Playbook and Policy  
Project Report**

*Created by:* ***Harsh Patel***

*Date:* ***January 23, 2025***

*Table of Contents*

*Executive Summary 3*

*Purpose 3*

*Incident Response Steps 3*

*Workflow Flowchart 5*

*Policies 6*

*Reference 7*

*Presentation 8*

**Executive Summary**

Ransomware attacks are a growing threat to organizations, often causing significant financial and reputational harm. This playbook provides a structured response to ransomware incidents, ensuring rapid containment, eradication, and recovery while minimizing impact. Aligned with the NIST Incident Response Lifecycle, it enables organizations to handle incidents efficiently and systematically. The playbook outlines actionable steps, assigns responsibilities, and integrates policies to enhance organizational resilience against ransomware threats.

**Purpose**

The purpose of this playbook is to provide a clear and actionable guide for responding to ransomware incidents. It ensures that all team members understand their roles and responsibilities, helping to protect organizational assets and maintain business continuity. This document also facilitates compliance with industry standards and regulatory requirements.

**Incident Response Steps**

**1. Preparation Phase**

**Actionable Steps:**

1. **Conduct Regular Backups:** Schedule daily, weekly, or monthly backups, depending on criticality. Use tools like **Veeam**, **Acronis Backup**, or cloud-based solutions. Verify backup integrity through test restores every quarter to ensure reliability.
2. **Implement Cybersecurity Awareness Training:** Provide periodic training to employees about phishing, social engineering, and safe internet usage. Simulate phishing attacks quarterly to gauge awareness.
3. **Establish and Test Incident Response Policies:** Review and update the incident response playbook annually. Conduct tabletop exercises and full-scale simulations to test readiness.

**Assigned To:** IT and Security Teams

**2. Identification Phase**

**Actionable Steps:**

1. **Monitor Network Activity:** Utilize SIEM tools like **Splunk** or **LogRhythm** to track unusual behaviors such as large file encryption or exfiltration. Set alerts for anomalies.
2. **Use Threat Intelligence Tools:** Integrate tools like **VirusTotal**, **AlienVault OTX**, or endpoint detection and response (EDR) tools like **CrowdStrike** to detect ransomware signatures.
3. **Isolate Suspected Infected Systems:** Quarantine systems showing signs of compromise using network access control (NAC) or manually disconnect them from the network.

**Assigned To:** SOC Analysts

**3. Containment Phase**

**Actionable Steps:**

1. **Disconnect Infected Systems:** Ensure compromised systems are removed from the network immediately to prevent the spread of ransomware.
2. **Apply Network Segmentation:** Reconfigure firewalls and VLANs to isolate critical systems and create zones to contain the infection.
3. **Notify Key Stakeholders:** Alert the Incident Response Team (IRT), management, and relevant departments promptly to ensure a coordinated response.

**Assigned To:** Network and IT Teams

**4. Eradication Phase**

**Actionable Steps:**

1. **Remove Malicious Files and Scripts:** Use antivirus tools like **ClamAV**, EDR platforms, or manual techniques (e.g., locating files in /tmp/, /var/, or user directories) to delete infected files.
2. **Patch Vulnerabilities:** Deploy patches for any vulnerabilities exploited by the ransomware. Use tools like **Nessus** or **OpenVAS** to identify unpatched systems and remediate them.

**Assigned To:** Incident Response Team

**5. Recovery Phase**

**Actionable Steps:**

1. **Restore Systems Using Verified Backups:** Use only pre-tested, uninfected backups to ensure a clean restoration. Validate the recovery with checksum comparisons.
2. **Conduct Thorough Testing:** After recovery, ensure all applications and systems are functioning correctly and check for potential re-infection signs.
3. **Monitor for Residual Threats:** Continue network monitoring post-recovery for indicators of compromise (IOCs) to ensure no reinfection occurs.

**Assigned To:** IT Teams

**6. Lessons Learned Phase**

**Actionable Steps:**

1. **Conduct a Post-Incident Review:** Analyze the incident timeline, affected systems, and response effectiveness. Identify gaps or weaknesses in current practices.
2. **Update Policies and Procedures:** Modify incident response plans, security policies, and employee training based on lessons learned.
3. **Share Insights with Stakeholders:** Prepare an executive-level report summarizing the incident, the response, and key takeaways. Present it to management and relevant teams to enhance organizational learning.

**Assigned To:** Incident Response Team and Management

**Command Lines**

1. **Analyze running processes:**

ps aux | grep suspicious\_process

**Explanation:**

* The ps aux command lists all running processes with details like process ID (PID), CPU/memory usage, user, and command name.
* grep suspicious\_process filters the output to search for a specific process name or keyword (suspicious\_process in this case).
* **Purpose:** Identifies malicious or unusual processes running on the system, such as ransomware or unauthorized scripts.
* **Why:** Analyzing processes helps pinpoint active threats that may need immediate termination or further investigation.

1. **Check network connections:**

netstat -antup | grep 443

**Explanation:**

* netstat -antup displays active network connections:
  + -a: Shows all connections.
  + -n: Displays addresses and ports in numeric form.
  + -t: Lists TCP connections.
  + -u: Lists UDP connections.
  + -p: Displays the associated program for each connection.
* grep 443 filters the results to show connections using port 443 (typically HTTPS traffic).
* **Purpose:** Helps identify suspicious or unauthorized traffic on critical ports.
* **Why:** Ensures the traffic is legitimate and not being exploited for data exfiltration or communication with command-and-control servers.

1. **Scan for malware:**

clamscan -r /path/to/directory

**Explanation:**

* clamscan is a command-line antivirus scanner provided by ClamAV.
* -r: Recursively scans all files in the specified directory.
* /path/to/directory: The target directory to be scanned for potential malware.
* **Purpose:** Detects and reports known malware signatures.
* **Why:** Scanning ensures compromised files are identified, aiding in containment and eradication efforts.

1. **Firewall rule updates:**

ufw deny from <IP\_ADDRESS>

**Explanation:**

* ufw (Uncomplicated Firewall) is a front-end for managing iptables on Linux systems.
* deny from <IP\_ADDRESS> blocks all incoming traffic from the specified IP address.
* **Purpose:** Prevents communication from a malicious IP address.
* **Why:** Blocking malicious IPs mitigates ongoing attacks and prevents further intrusion attempts.

**5. Memory Analysis:**

vol.py -f memory.dump --profile=Win10x64 malfind

**Explanation:**

* vol.py: Refers to Volatility, a popular memory forensics tool.
* -f memory.dump: Specifies the memory dump file to analyze.
* --profile=Win10x64: Indicates the operating system profile (e.g., Windows 10, 64-bit).
* malfind: Runs the malfind plugin to identify suspicious memory regions associated with malware.
* **Purpose:** Analyzes memory dumps for signs of malicious activity.
* **Why:** Memory analysis reveals in-memory malware or processes not visible in file systems, aiding deep forensic investigations.

**6. Forensic Disk Imaging:**

dd if=/dev/sdX of=/path/to/image.img bs=4M status=progress

**Explanation:**

* dd: A low-level data copying tool.
* if=/dev/sdX: Specifies the input file (source disk or partition).
* of=/path/to/image.img: Specifies the output file (destination for the disk image).
* bs=4M: Sets the block size to 4 MB for faster copying.
* status=progress: Displays the copy progress in real-time.
* **Purpose:** Creates an exact bit-by-bit image of a storage device for forensic analysis.
* **Why:** Ensures the integrity of digital evidence while preserving the original data for legal or investigative purposes.

**File Locations**

**1. Backup Files: /mnt/backup/**

**Explanation:**

* This directory stores critical system and data backups.
* Backups are essential for recovering from ransomware attacks, as they provide a clean, unaltered version of data and systems.
* **Security Measures:**
  + Access is restricted to system administrators only, using strict file permissions (chmod and chown).
  + Encrypted storage ensures that backup data cannot be accessed without the proper decryption keys.

Ransomware incidents often involve encrypting or deleting data, so having reliable, offline backups is vital for recovery.

**2. Incident Logs: /var/logs/incidents/**

**Explanation:**

* This directory contains logs related to detected incidents, including timestamps, actions taken, and related alerts.
* Logs are critical for identifying patterns, understanding the scope of an attack, and supporting forensic investigations.
* **Security Measures:**
  + Logs are stored with write-only access for logging services and read-only access for investigators.
  + Logs are protected against tampering using hashing mechanisms, such as SHA-256 checksums, to verify integrity.
  + A log management system, like a SIEM, aggregates and monitors these logs in real-time.

Logs serve as a timeline and evidence for incident response and compliance with regulations.

**3. Evidence Storage: /secure/evidence/**

**Explanation:**

* This directory is used for storing digital evidence collected during an investigation, such as memory dumps, disk images, and malware samples.
* Evidence is critical for internal investigations, legal proceedings, and reporting to regulatory authorities.
* **Security Measures:**
  + This directory is on a physically and logically isolated storage system to prevent unauthorized access.
  + Files are encrypted during storage and transfer to maintain confidentiality and integrity.
  + A robust audit trail is maintained, tracking who accessed the directory and for what purpose.
  + Evidence is collected systematically using tools like dd for disk images or tcpdump for network traffic.
  + Each piece of evidence is labeled with metadata, including the case ID, collection date, and responsible investigator.
  + Chain-of-custody forms are maintained to document who accessed or handled the evidence, ensuring its admissibility in court.

Ensures the preservation, integrity, and admissibility of evidence for legal and investigative purposes.

**Workflow Flowchart**

Step 1  
Preparation  
Develop IR Plan, train staff etc.

Step 6   
Post Incident  
Conduct incident Review and Document Findings

Step 3   
Containment  
Isolate infected systems

Step 5   
Recovery  
Restore from Back Up, Test Systems

Step 4   
Eradication  
Remove Ransomware, Patch Vulnerabilities

Step 2  
identification  
Detect and Confirm Ransomware

**Policies**

**Policy 1: Malware Outbreak Policy**

* **Purpose:** To ensure a standardized and efficient response to malware outbreaks, limiting potential damage and ensuring quick recovery.
* **Importance:** Malware outbreaks can disrupt operations, compromise sensitive information, and propagate throughout the organization’s network if not managed effectively.
* **Activities:**
  + Conduct weekly scans using **ClamAV**, **Malwarebytes**, or **Windows Defender** (depending on the OS).
  + Investigate and quarantine any files flagged as suspicious during scans. Escalate findings to the IT Security team.
  + Isolate affected systems from the network immediately upon malware detection to prevent lateral movement.
  + Keep antivirus tools and signatures up to date and validate their configuration monthly.
* **Playbook Reference:** Aligned with Identification, Containment, and Eradication stages.
* **Consequences of Non-Compliance:**
  + **For Individuals:** May result in restricted system access, mandatory training, or disciplinary action.
  + **For the Company:** Increased risk of widespread infection, operational downtime, and reputational harm.

**Policy 2: Data Breach Policy**

* **Purpose:** To mitigate and manage incidents involving unauthorized access or disclosure of personally identifiable information (PII) or other sensitive data.
* **Importance:** Protecting sensitive data is critical to maintaining trust, meeting regulatory requirements (e.g., GDPR, CCPA), and avoiding financial penalties.
* **Activities:**
  + Review access logs daily using tools like **Splunk**, **Graylog**, or **ELK Stack** for signs of unauthorized access.
  + Focus on critical logs such as:
    - Privileged user activity.
    - Remote access connections.
  + Notify the in charge officer and affected stakeholders within 24 hours of breach detection, as required by GDPR or similar laws.
  + Collaborate with the Legal and Public Relations teams to manage breach notifications.
* **Playbook Reference:** Primarily aligns with the Identification and Notification stages.
* **Consequences of Non-Compliance:**
  + **For Individuals:** Potential termination or legal action for negligence.
  + **For the Company:** Regulatory fines, loss of customer trust, and reputational damage.

**Policy 3: Data Retention and Destruction Policy**

* **Purpose:** To manage the lifecycle of organizational data responsibly, ensuring secure retention and timely, compliant disposal of data.
* **Importance:** Minimizing the storage of unnecessary or outdated data reduces risk, cost, and compliance burden while protecting sensitive information.
* **Activities:**
  + Conduct quarterly audits of data storage systems to ensure compliance with retention policies.
  + Retain data only as long as necessary for business or regulatory purposes (e.g., follow HIPAA or GDPR requirements for medical or personal data).
  + Securely delete data that has reached the end of its retention period using tools like:
    - shred or srm for Linux-based systems.
    - BleachBit or built-in BitLocker wiping for Windows systems.
    - AWS S3 Object Lock for cloud-based storage.
  + Maintain a log of all data destruction activities, including the date, responsible personnel, and verification of deletion.
* **Playbook Reference:** Recovery and Lessons Learned stages to ensure data is not mishandled during and after incidents.
* **Consequences of Non-Compliance:**
  + **For Individuals:** Legal and disciplinary action, including termination.
  + **For the Company:** Exposure of sensitive data, regulatory fines, and legal consequences.

**Policy 4: Remote Work Security Policy**

* **Purpose:** To safeguard company assets and sensitive information while employees work remotely.
* **Key Activities:**
  + Use company-approved VPNs and endpoint protection solutions.
  + Prohibit the use of personal devices for work-related tasks unless explicitly authorized.
  + Mandate regular updates and patches for remote systems.

**Policy 5: Password Management Policy**

* **Purpose:** To enforce robust password security practices across the organization.
* **Key Activities:**
  + Require employees to use a password manager and enforce complex, unique passwords.
  + Implement multi-factor authentication (MFA) for all critical systems.
  + Require password changes every 90 days, with minimum length and complexity requirements.

References

Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Digital Transformation Service Sector & Digital Transformation Service Sector. (2021, December 8). *Develop an Incident Response Plan: Fillable template and example*. <https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example>

Cybersecurity and Infrastructure Security Agency. (2021). *Cybersecurity Incident & Vulnerability Response Playbooks*. <https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>

Cichonski, P., Millar, T., Grance, T., Scarfone, K., National Institute of Standards and Technology, United States Computer Emergency Readiness Team, & Scarfone Cybersecurity. (2012). Computer Security Incident Handling Guide. In *NIST Special Publication 800-61* (Revision 2). <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

FRSecure. (2023, August 15). *Incident Response Plan Template | FRSecure*. FRSecure. <https://frsecure.com/incident-response-plan-template/>

Enaohwo, O. M. (2024, December 29). *How to write a policy for your business and employees*. SweetProcess. <https://www.sweetprocess.com/how-to-write-a-policy/#:%7E:text=A%20policy%20is%20simply%20a,is%20your%20organization's%20action%20plan>

**Presentation**

**A white cover with black lines

Description automatically generated**

**A black and white background with white lines

Description automatically generated**

**A close-up of a document

Description automatically generated**

**A close-up of a computer screen

Description automatically generated**

**A close-up of a padlock

Description automatically generated**

**A close-up of a playbook

Description automatically generated**

**A white background with text and lines

Description automatically generated**

**A white and black text on a white background

Description automatically generated**

**A close-up of a document

Description automatically generated**

**A black background with white text

Description automatically generated**

**A black background with white text

Description automatically generated**