Incident Response Playbook Plan for Ransomware

This playbook will cover the following phases of incident response:

- Preparation: Steps to prepare for potential incidents.
- Detection and Analysis: How to detect and analyze the incident.
- Containment: Steps to contain the incident and prevent further damage.
- Eradication: How to eliminate the root cause of the incident.
- Recovery: Steps to restore normal operations.
- Post-Incident Activity: Lessons learned and improvements.

Step 1: Define the Hypothetical Scenario

Let's assume the following scenario:

- Attack Type: Ransomware attack.
- Target: A small business network.
- Impact: Critical files encrypted, systems offline, and ransom demand.

Step 2: Create the Incident Response Playbook

Here's the detailed playbook for the ransomware attack:

1. Preparation

*** Team Roles and Responsibilities:**

1. Incident Manager: Oversees the response process.
2. IT Team: Handles technical containment and recovery.
3. Legal Team: Advises on compliance and legal implications.
4. PR Team: Manages communication with stakeholders.

*** Tools and Resources:**

1. Antivirus software, firewalls, and intrusion detection systems (IDS).
2. Backup systems and disaster recovery plans.
3. Contact list for law enforcement and cybersecurity experts.

*** Training and Drills:**

1. Conduct regular incident response drills.
2. Train employees on ransomware awareness.

2. Detection and Analysis

*** Detection:**

1. Monitor for unusual activity (e.g., file encryption, ransom notes).
2. Use IDS and antivirus software to detect ransomware.

*** Analysis:**

1. Identify the ransomware variant (e.g., WannaCry, LockBit).
2. Determine the scope of the attack (e.g., affected systems, encrypted files).
3. Collect evidence (e.g., logs, ransom note).

3. Containment

*** Short-Term Containment:**

1. Isolate infected systems from the network.
2. Disable shared drives and remote access.

*** Long-Term Containment:**

1. Apply patches to vulnerable systems.
2. Update firewall rules to block malicious IPs.

4. Eradication

*** Remove Malware:**

1. Use antivirus software to remove ransomware.
2. Rebuild infected systems from clean backups.
3. Eliminate Root Cause:
4. Identify and patch vulnerabilities (e.g., unpatched software, weak passwords).
5. Disable compromised user accounts.

5. Recovery

*** Restore Systems:**

1. Restore encrypted files from backups.
2. Verify the integrity of restored files.

*** Monitor for Recurrence:**

1. Continuously monitor systems for signs of reinfection.
2. Conduct a full system scan.

6. Post-Incident Activity

*** Lessons Learned:**

1. Conduct a post-incident review with the response team.
2. Identify gaps in the response process.

*** Improvements:**

1. Update the incident response plan based on lessons learned.
2. Implement additional security measures (e.g., multi-factor authentication, regular backups).

Step 3: Format the Playbook

Here's how to structure the playbook in a professional format: Incident Response Playbook for Ransomware Attacks

1. Preparation

*** Team Roles and Responsibilities:**

1. Incident Manager: [Name]
2. IT Team: [Names]
3. Legal Team: [Names]
4. PR Team: [Names]

*** Tools and Resources:**

1. Antivirus: [Software Name]
2. Backup System: [System Name]
3. Contact List: [Attach Contact List]

*** Training and Drills:**

1. Conduct drills every [frequency].

2. Detection and Analysis

*** Detection:**

1. Monitor for [specific signs of ransomware].
2. Use [specific tools] to detect ransomware.

*** Analysis:**

1. Identify ransomware variant: [steps].
2. Determine scope: [steps].
3. Collect evidence: [steps].

3. Containment

*** Short-Term Containment:**

1. Isolate systems: [steps].
2. Disable shared drives: [steps].

*** Long-Term Containment:**

1. Apply patches: [steps].
2. Update firewall rules: [steps].

4. Eradication

*** Remove Malware:**

1. Use [antivirus software] to remove ransomware.
2. Rebuild systems: [steps].

*** Eliminate Root Cause:**

1. Patch vulnerabilities: [steps].
2. Disable compromised accounts: [steps].

5. Recovery

*** Restore Systems:**

1. Restore files: [steps].
2. Verify integrity: [steps].

*** Monitor for Recurrence:**

1. Continuous monitoring: [steps].
2. Full system scan: [steps].

6. Post-Incident Activity

*** Lessons Learned:**

1. Conduct review: [steps].
2. Identify gaps: [steps].

*** Improvements:**

1. Update response plan: [steps].
2. Implement additional measures: [steps].

Step 4: Create a Sample Playbook Document

Here’s a sample playbook document for the ransomware scenario:
Incident Response Playbook for Ransomware Attacks

1. Preparation

*** Team Roles and Responsibilities:**

1. Incident Manager: John Doe
2. IT Team: Jane Smith, Alex Brown
3. Legal Team: Sarah Lee
4. PR Team: Emily Davis

*** Tools and Resources:**

1. Antivirus: Windows Defender
2. Backup System: Acronis Backup
3. Contact List: [Attach Contact List]

*** Training and Drills:**

1. Conduct drills every 6 months.

2. Detection and Analysis

*** Detection:**

1. Monitor for file encryption and ransom notes.
2. Use Windows Defender and IDS to detect ransomware.

*** Analysis:**

1. Identify ransomware variant using VirusTotal.
2. Determine scope by checking affected systems and files.
3. Collect logs and ransom note for evidence.

3. Containment

*** Short-Term Containment:**

1. Isolate infected systems by disconnecting them from the network.
2. Disable shared drives and remote access.

*** Long-Term Containment:**

1. Apply patches to vulnerable systems.
2. Update firewall rules to block malicious IPs.

4. Eradication

*** Remove Malware:**

1. Use Windows Defender to remove ransomware.
2. Rebuild infected systems from clean backups.

*** Eliminate Root Cause:**

1. Patch vulnerabilities in unpatched software.
2. Disable compromised user accounts.

5. Recovery

*** Restore Systems:**

1. Restore encrypted files from Acronis Backup.
2. Verify the integrity of restored files.
3. Monitor for Recurrence:
4. Continuously monitor systems for signs of reinfection.
5. Conduct a full system scan using Windows Defender.

6. Post-Incident Activity

*** Lessons Learned:**

1. Conduct a post-incident review with the response team.
2. Identify gaps in the response process.

*** Improvements:**

1. Update the incident response plan based on lessons learned.
2. Implement multi-factor authentication and regular backups.

Step 5: Test the Playbook

1. Simulate a ransomware attack in a controlled environment.
2. Follow the playbook step by step.
3. Identify any gaps or areas for improvement.