Ransomware Incident Response

Purpose

This procedure outlines the steps to be taken in the event of a ransomware attack. Using the SANS and Blumira incident response framework as a baseline, a 7 Phase of Incident Response: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned, and Post-Incident Activities was developed [1] [2]. This procedure aims to minimize the impact of ransomware incidents to protect the Abel organization's data and systems, and to ensure business continuity. The scope of this incident response plan and the definition of terms can be found at the appendices page (appendix 1 and appendix 2).

Incident Response Plan: The Communication Hierarchy can be found at the appendices page (appendix 3)

Step 1: Preparation

Objective: To establish a proactive stance and prepare for potential ransomware attacks.

- **Policy:** Develop a comprehensive incident response policy that defines the principles, rules, and practices of the organization to guide security processes. Ensure the policy is highly visible to employees and users, and clearly states unauthorized activities and associated penalties.
- **Response Plan/Strategy:** Create a plan for incident handling, prioritizing incidents based on organizational impact. Consider factors like the number of employees affected, revenue impact, and sensitive data involvement.
- **Communication:** Establish a communication plan that defines which IRT members to contact during an incident, for what reasons, and when. Include procedures for contacting law enforcement and stakeholders.
- **Documentation:** Ensure thorough documentation of incidents, including who, what, when, where, why, and how. This documentation will be crucial for incident response, lessons learned, and potential legal action.

- **Team:** Build a diverse IRT team with relevant skills, including security, IT operations, legal, human resources, and public relations.
- **Access Control:** Ensure IRT staff have appropriate permissions to perform their duties. Network administrators should add permissions to IRT member accounts and remove them when the incident is resolved.
- **Training and Awareness:** Provide training and awareness programs for employees and stakeholders on incident response and security best practices.
- **Tools:** Evaluate, select, and deploy software and hardware tools to aid in incident response. Package these tools in a "jump bag" for quick access during incidents.

Step 2: Identification

Objective: Detect and confirm the occurrence of a ransomware attack.

- **Monitoring:** Set up monitoring for all sensitive IT systems and infrastructure.
- **Analysis:** Analyze events from multiple sources, including log files, error messages, and security tool alerts.
- **Incident Identification:** Correlate data from multiple sources to identify incidents and report them promptly.
- **Notification:** Encourage employees to notify IRT members of any anomalies and establish communication with the IT helpdesk and a designated command center.
- **Documentation:** Document everything incident responders do during the incident, answering who, what, where, why, and how questions.

Step 3: Containment

Objective: Limit the spread and impact of the ransomware.

- **Short-term Containment:** Limit damage by isolating network segments, taking down hacked production servers, and routing to failover.
- **System Backup:** Take a forensic image of affected systems with tools like FTK or EnCase, then wipe and reimage the systems.

- **Long-term Containment:** Apply patches and review firewall settings to bring production systems back up. Remove attacker accounts or backdoors, restrict network access to limit further exposure, and address root causes.

Step 4: Eradication

Objective: Remove ransomware from the infected systems and eliminate the root cause.

- **Reimaging:** Completely wipe and reimage affected system hard drives to remove malicious content.
- **Root Cause:** Understand and address the incident's root cause to prevent future compromise.
- **Security Best Practices:** Apply basic security best practices, such as upgrading old software versions and disabling unused services.
- **Malware Scan:** Use anti-malware software or Next-Generation Antivirus (NGAV) to scan affected systems and ensure all malicious content is removed.

Step 5: Recovery

Objective: Restore systems and data to normal operations.

- **Restore Data:** Recover data from backups, ensuring that backups are uncompromised.
- **Test and Verify:** Ensure systems are clean and fully functional before going live.
- **Monitoring:** Ongoing monitoring for abnormal behaviors after the incident.
- **Prevention:** Consider measures to protect restored systems from the recurrence of the same incident.

Step 6: Lessons Learned

Objective: Review the incident and improve future response efforts.

- Documentation: Complete documentation of the incident to identify lessons for next time.
- Incident Report: Publish a comprehensive incident report, including a play-by-play review, who, what, where, why, and how questions.

- IRT Performance Improvement: Extract items from the incident report that can be improved for next time.
- Benchmarking: Derive metrics from the incident report to guide future incidents.
- Lessons Learned Meeting: Conduct a meeting with the IRT team and stakeholders to discuss the incident and cement lessons learned.

Step 7: Post-Incident Activities

Objective: Turn the incident into an opportunity for growth.

- **Reporting:** Prepare a detailed report for internal stakeholders and report the incident to external parties as required.
- **Review and Refine:** Review the incident response plan and refine it based on lessons learned.
- **Incident Response Plan Update:** Update the incident response plan to reflect changes in the organization, technology, and threat landscape.
- **Re-testing:** Test the newly patched systems to ensure the malware is gone and can't be restored.

References

[1] Cynet, "Incident Response SANS: The 6 Steps in Depth," Cynet Security, LTD, 2024. [Online]. Available: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/. [Accessed 22 May 2024].

[2] E. Eubanks, "Incident Response Strategies for Ransomware," Blumira, 30 October 2023. [Online]. Available: https://www.blumira.com/incident-response-ransomware/. [Accessed 22 May 2024].

Appendices

Appendix 1: Scope

This report aims to provide Abel organization with a structured approach to handle and recover from a ransomware attack. These includes:

1. Detailed steps for each of the 7 Phases of Incident Response.
2. A communication hierarchy to ensure effective incident management.
3. Roles and responsibilities of the Incident Response Team.
4. Definitions of key terms related to ransomware attacks.
5. References to relevant sources and best practices.

Appendix 2: Definition of terms

- **Ransomware**: Malicious software that encrypts data on a victim's system, demanding payment for decryption.
- **Incident Response Plan (IRP)**: A documented strategy with steps to manage and respond to security incidents, including ransomware attacks.
- **Encryption**: The process of converting data into code to prevent unauthorized access.
- **Backup**: A copy of data stored separately from the original to be used in case the original is lost or compromised.
- **Malware**: Software designed to disrupt, damage or gain unauthorized access to computer systems.

Appendix 3: Communication Hierarchy

1. Incident Response Coordinator (IRC)
2. Chief Information Security Officer (CISO)
3. IT Security Team Lead
4. IT Operations Team Lead
5. Legal and Compliance Officer
6. Public Relations Officer
7. HR Manager

Step 1: preparation

Responsible: Chief Information Security Officer (CISO), Human Resources (HR) Manager, and IT Security Team Lead.

Step 2: Identification

Responsible: IT Security Team and employees

Step 3: Containment

Responsible: IT Operations Team and IT Security Team

Step 4: Eradication

Responsible: IT Security Team

Step 5: Recovery

Responsible: IT Operations Team and IT Security Team

Step 6: Lesson learned

Responsible: Incident Response Coordinator (IRC) and CISO

Step 7: Post-incident activities

Responsible: IRC, Legal and Compliance Officer, and Public Relations Officer

Safeguarding the Incident Response Plan

The Incident Response Plan should be maintained and safeguarded by the Chief Information Security Officer (CISO). The CISO ensures the plan is regularly reviewed, updated and tested through drills and tabletop exercises. Access to the plan should be restricted to key members of the Incident Response Team and senior management.