Advanced Cyber Incident Response Plan

Organization: Internee.pk

Executive Summary

This document presents a comprehensive Cyber Incident Response Plan (CIRP) designed to manage, contain, and recover from cybersecurity incidents. It follows industry-recognized practices and enhances organizational readiness against ransomware, malware, phishing, and data breach incidents.

1. Incident Response Framework

The Incident Response lifecycle consists of six strategic phases: Preparation, Identification, Containment, Eradication, Recovery, and Post-Incident Review. Each phase ensures structured coordination and risk reduction.

- Preparation: Establish response team, tools, policies, backups, and training.
- Identification: Detect and validate incidents through logs, SIEM alerts, and reports.
- Containment: Isolate systems and block malicious activity.
- Eradication: Remove malware, patch vulnerabilities, reset credentials.
- Recovery: Restore operations from verified backups and monitor stability.
- Post-Incident Review: Document findings and enhance security controls.

2. Simulated Ransomware Attack Scenario

Scenario: A phishing email disguised as an invoice infects an employee workstation. Ransomware encrypts files and attempts lateral movement across shared drives.

- Encrypted and inaccessible files.
- Operational downtime and service disruption.
- Potential financial and reputational damage.
- Risk of data exposure if exfiltration occurs.

Response Actions: Immediate isolation of infected systems, account suspension, malware removal, restoration from offline backups, and enhanced monitoring.

3. Risk Mitigation & Security Enhancements

- Implementation of Multi-Factor Authentication (MFA).
- Regular vulnerability scanning and patch management.
- Email security filtering and phishing simulations.
- Network segmentation to prevent lateral movement.
- Continuous logging and SIEM monitoring.

Continuous staff training and tabletop exercises ensure preparedness for real-world cyber emergencies.

4. Conclusion

A structured Cyber Incident Response Plan significantly reduces the impact of cybersecurity incidents. Through preparation, timely detection, strategic containment, and systematic recovery, Internee.pk can maintain business continuity and protect critical assets.