Incident Response Playbooks for Redback Operations

Attacks

Denial of Service (DoS) Attack Playbook:

Preparation:
Documentation: Make a list of critical services and their expected behaviour.
Monitoring Tools: Implement network traffic and service availability monitoring solutions.
Response Team: Assign roles and responsibilities for immediate response.

Identification:
Identify sudden spikes in network traffic or service outages.
Analyze Traffic: Identify the source and type of the DoS attack.

Notification:
Internal Alert: Notify the incident response team and any other stakeholders who may be affected.
Service Users: Notify users of potential service disruptions and expected resolutions.

Containment:
Filtering traffic: Use filters or firewall rules to prevent malicious traffic.
Service Rerouting: Reroute legitimate traffic away from affected systems.

Eradication:
Analyse Attack: Investigate the attack vectors to learn about vulnerabilities.
Implement Countermeasures: To prevent future attacks, install patches or configure your system.

Recovery:
Service Restoration: Gradually restore affected services after ensuring the attack is mitigated.
System Checks: Verify the integrity of affected systems and data.

Post-Incident:
Lessons Learned: Conduct a post-incident investigation and document your findings.
Enhancements: Make security improvements to prevent similar attacks in the future.

Phishing Attack Playbook:

Preparation:
Training: Conduct regular phishing awareness training for employees.
Email Filtering: Use email filtering solutions to detect phishing emails.

Identification:
Employee Reports: Encourage employees to promptly report suspicious emails.
Email Analysis: Examine reported emails for phishing indicators.

Notification:
Internal Alert: Notify the incident response team and affected employees immediately.
User Awareness: Educate employees about the phishing attack and precautionary measures.

Containment:

Isolation: Isolate affected systems to prevent further compromise.
Password Resets: Begin password resets for affected accounts.

Eradication:

Email Blacklisting: Blacklist sender domains or addresses associated with the phishing campaign.
Security Updates: Ensure all systems are updated with the latest security patches.

Recovery:
System Checks: Scan systems for any malware or unauthorized access.
User Training: Reinforce phishing awareness and best practices.

Post-Incident:
Analysis: Review the incident to identify weaknesses in security measures.
Enhancements: Implement improvements in email filtering and employee training.

Ransomware Attack Playbook:

Preparation:
Backup Strategy: Establish and maintain regular backups of critical data.
Security Software: Implement robust antivirus and anti-ransomware solutions.
Employee Training: Educate employees on recognizing suspicious files or links.

Identification:
Anomaly Detection: Monitor for unusual file changes or encryption activities.
Ransom Note: Identify and analyze ransom notes or indicators of compromise.

Notification:
Immediate Alert: Notify the incident response team and affected stakeholders.
Isolation: Disconnect affected systems from the network to prevent further encryption.

Containment:
Identify Scope: Assess the extent of encrypted files and affected systems.
Quarantine: Isolate infected systems to contain the spread.

Eradication:
Malware Removal: Utilize antivirus tools to remove ransomware from affected systems.
Data Recovery: Restore encrypted data from backups.

Recovery:
System Restoration: Gradually restore affected systems after ensuring malware removal.
Security Checks: Perform security checks to prevent reinfection.

Post-Incident:
Review Backup Policy: Assess backup frequency and integrity.
Enhancements: Strengthen security measures to prevent future ransomware attacks.

Malware Attack Playbook:

Preparation:
Security Software: Implement robust antivirus and malware detection solutions.
Employee Education: Train employees on safe browsing and downloading practices.

Identification:
Anomaly Detection: Monitor for suspicious behavior or file changes.
Antivirus Alerts: Respond to antivirus alerts indicating potential malware.

Notification:
Internal Alert: Notify the incident response team and relevant stakeholders.
System Isolation: Isolate infected systems from the network.

Containment:
Malware Quarantine: Quarantine infected files or systems to prevent further spread.
Access Control: Limit user access to prevent malware propagation.

Eradication:
Malware Removal: Use antivirus tools to eradicate malware from affected systems.
Patch and Update: Apply patches to address vulnerabilities exploited by the malware.

Recovery:
System Restoration: Gradually restore affected systems after malware removal.
User Training: Reinforce training on malware prevention.

Post-Incident:
Analysis: Review the incident for lessons learned and identify security gaps.
Enhancements: Improve malware detection and prevention measures.

Data Breach Playbook:

Preparation:
Data Classification: Classify and prioritize sensitive data for protection.
Access Control: Implement strict access controls and encryption measures.

Identification:
Anomaly Detection: Monitor for unauthorized access or unusual data transfers.
Data Audit: Analyze logs and databases for potential breaches.

Notification:
Immediate Alert: Notify the incident response team and relevant authorities.
Affected Parties: Inform individuals affected by the breach.

Containment:
Data Segmentation: Isolate compromised data to prevent further access.
System Lockdown: Secure affected systems to prevent additional breaches.

Eradication:
Vulnerability Patching: Address vulnerabilities that led to the breach.
Data Restoration: Restore affected data from secure backups.

Recovery:
Compliance Check: Ensure compliance with data protection regulations.
Incident Review: Conduct a review to prevent similar breaches.

Post-Incident:
Security Enhancements: Strengthen security measures based on the breach analysis.
Communication Strategy: Develop communication plans for future breaches.

Industrial Control System Compromise Playbook:

Preparation:
Segmentation: Segment ICS networks from external networks for added security.
Regular Audits: Conduct regular security audits and assessments of ICS systems.

Identification:
Anomaly Detection: Monitor for unusual activities or commands in the ICS environment.
Behavior Analysis: Analyze ICS behavior for deviations from normal operations.

Notification:
Immediate Alert: Notify the incident response team and ICS personnel.
System Isolation: Isolate compromised ICS systems to prevent further damage.

Containment:
Disabling Access: Disable compromised control systems or segments.
Backup Systems: Activate backup systems if available.

Eradication:
Malware Removal: Remove malware or unauthorized software from ICS systems.
Security Updates: Apply patches and updates to secure vulnerabilities.

Recovery:
System Restoration: Gradually restore ICS functionality after ensuring security measures.
Testing: Test restored systems for functionality and security.

Post-Incident:
Analysis and Review: Conduct a thorough review of the incident for ICS security improvements.
Training and Preparedness: Provide training on incident response for ICS personnel.

Vectors

External/Removable Media Vector Playbook:

Preparation:
Policy Development: Create policies for the use of external media devices.
Security Software: Endpoint security software should be used to scan and monitor external media.

Identification:
Monitoring: Regularly scan systems for connected external media devices.
Anomaly Detection: Identify unusual file transfers or unauthorised access.

Notification:

Alert System: Set up alerts for the incident response team when unauthorised media access is detected.
User Awareness: Educate users on the dangers of using external media.

Containment:
Disconnecting Media: Separate the affected systems from the external media device.
Access Control: To prevent further data transfer, restrict access.

Eradication:
Malware Scans: Scan affected systems for malware.
Policy Review: Policy for external media usage should be evaluated and updated.

Recovery:
System Restoration: Clean backups should be used to restore affected systems.
User Training: Reinforce training on safe use of external media.

Post-Incident:
Policy Enhancement: Based on incident analysis, strengthen policies governing the use of external media.
Monitoring Improvements: Improve monitoring for external media access.

Attrition Vector Playbook:

Preparation:
Asset Inventory: Keep an up-to-date inventory of critical assets.
Backup Strategy: Back up critical data and assets on a regular basis..

Identification:
Monitoring: Keep an eye on systems for unusual attrition or data deletion.
Audit Trails: Examine logs for evidence of unauthorised access or data deletion attempts.

Notification:
Immediate Alert: Notify the incident response team and any stakeholders who are affected.
Data Loss Analysis: Determine the extent and impact of the data loss.

Containment:
Halting Attrition: Isolate affected systems to prevent further data loss.
Access Control: Limit access to avoid further attrition.

Eradication:
Data Recovery: Attempt to recover lost data from backups or sources.
System Checks: Perform integrity checks on the affected systems.

Recovery
Data Restoration: Gradually restore lost data after ensuring the security of systems.
Training and Awareness: Users should be educated on data security best practices.

Post-Incident:
Review and Analysis: Conduct a post-mortem investigation to avoid future attrition incidents.
Enhancements: Enhance security measures to prevent unauthorized data deletion.

Web Vector Playbook:

Preparation:
Web Filtering: Implement web filtering tools to block malicious sites.
Browser Security: Enforce secure browser settings and plugins.

Identification:
Anomaly Detection: Examine web traffic for suspicious or unauthorised activity.
Behavior Analysis: Examine user behaviour for signs of web-based threats.

Notification:
Alert System: Notify the incident response team upon detecting suspicious web activities.
User Awareness: Educate users about safe browsing habits.

Containment:
Blocking Access: Block access to suspicious or compromised websites.
Quarantine Systems: To prevent further compromise, isolate affected systems.

Eradication:
Malware Scans: Perform scans for malware or web-based threats on affected systems.
Patch Management: Apply patches to address vulnerabilities discovered via web vectors.

Recovery:
System Restoration: Gradually restore affected systems after malware removal and patching.
User Training: Reinforce training on safe web browsing practices.

Post-Incident:
Analysis and Review: Review the incident to enhance web security measures.
Continuous Monitoring: Implement enhanced web-based threat monitoring.

Email Vector Playbook:

Preparation:
Email Filtering: Deploy email filtering solutions to detect and block phishing attempts.
Employee Training: Conduct regular phishing awareness training for employees.

Identification:
Employee Reports: Encourage employees to report suspicious emails promptly.
Email Analysis: Analyze reported emails for phishing or malware indicators.

Notification:
Internal Alert: Notify the incident response team and affected users.
User Education: Inform users about the email-based threat and precautionary measures.

Containment:
Isolation: Isolate affected systems to prevent further compromise.
Password Resets: Initiate password resets for compromised accounts.

Eradication:
Email Blacklisting: Blacklist sender domains or addresses linked to the threat.
Security Updates: Apply patches to address vulnerabilities exploited through email.

Recovery:

System Checks: Examine systems for malware and unauthorised access..
Training Reinforcement: Reinforce training on email security best practices.

Post-Incident:
Review and Analysis: Analyze the incident to enhance email security measures.
Training Enhancement: Improve employee training based on incident findings.

Supply Chain Interdiction Vector Playbook:

Preparation:
Vendor Assessment: Assess and monitor the security posture of third-party vendors.
Contractual Requirements: Establish security requirements in contracts with suppliers.

Identification:
Monitoring: Monitor supply chain connections and activities for anomalies.
Supplier Communication: Communicate and verify with suppliers in case of suspicious activities.

Notification:
Incident Response Team: Notify the team about suspected supply chain interdiction.
Supplier Notification: Inform affected suppliers and collaborate on containment.

Containment:
Isolation: Isolate affected systems or components in the supply chain.
Alternative Sourcing: Identify alternative suppliers to mitigate disruptions.

Eradication:
Investigation: Investigate the root cause within the supply chain.
Security Updates: Apply patches or updates to secure affected systems.

Recovery:
Supply Chain Restoration: Gradually reintegrate verified supply chain components.
Monitoring: Check the security of the restored supply chain elements.

Post-Incident:
Supplier Review: Conduct a thorough review of supplier security practices.
Supply Chain Strengthening: Implement measures to fortify the supply chain against interdiction.

Impersonation Vector Playbook:

Preparation:
Authentication Measures: Implement multi-factor authentication to prevent impersonation.
Employee Training: Train employees to recognize and report impersonation attempts.

Identification:
Anomaly Detection: Monitor for unusual user access patterns or attempts.
Behavior Analysis: Analyze user behavior for signs of unauthorized access.

Notification:
Incident Response Team: Notify the team about suspected impersonation attempts.
User Awareness: Educate users about potential impersonation threats.

Containment:

Account Lockdown: Disable compromised accounts to prevent further access.
Access Review: Review access logs and permissions for irregularities.

Eradication:
User Verification: Verify compromised accounts and restore access securely.
Security Checks: Ensure no unauthorized changes were made during the incident.

Recovery:
System Checks: Perform system checks to ensure no lingering threats.
Training Reinforcement: Reinforce training on recognizing and reporting impersonation.

Post-Incident:
Analysis and Review: Analyze the incident to strengthen measures against impersonation.
Continuous Monitoring: Enhance monitoring for potential impersonation threats.

Improper Usage Vector Playbook:

Preparation:
User Policies: Establish clear policies on acceptable use of resources and systems.
Monitoring Tools: Implement monitoring solutions to detect policy violations.

Identification:
Anomaly Detection: Monitor for unusual or unauthorized activities on systems.
Policy Violation Analysis: Analyze logs for indications of improper usage.

Notification:
Incident Response Team: Notify the team about detected improper usage incidents.
User Education: Inform users about policy violations and their consequences.

Containment:
Access Control: Restrict access to systems involved in improper usage.
User Suspension: Suspend user privileges if necessary to prevent further violations.

Eradication:
Investigation: Investigate the root cause and extent of improper usage.
Policy Review: Review and update policies to prevent future violations.

Recovery:
System Checks: Ensure systems are free from unauthorized changes or data loss.
User Training: Reinforce training on proper system and resource usage.

Post-Incident:
Policy Enhancement: Enhance policies based on incident analysis to prevent future improper usage.
Monitoring Improvements: Strengthen monitoring for policy violations.

Loss/Theft of Equipment Vector Playbook:

Preparation:
Asset Management: Maintain an inventory of all equipment with sensitive data.
Encryption Measures: Encrypt sensitive data on portable devices.

Identification:

Inventory Audits: Regularly audit equipment inventory for discrepancies.
Tracking Tools: Use tracking solutions to identify lost or stolen equipment.

Notification:
Immediate Alert: Notify the incident response team and relevant stakeholders.
Data Assessment: Evaluate the potential impact of lost or stolen equipment.

Containment:
Remote Wipe: Remotely wipe data from lost or stolen devices if possible.
Access Control: Change access credentials to prevent unauthorized access.

Eradication:
Recovery Attempts: Attempt recovery or tracking of lost equipment.
Security Updates: Apply security updates or patches to prevent data breaches.

Recovery:
Data Restoration: Restore lost data from backups or alternative sources.
Policy Review: Review and update policies on equipment handling and data security.

Post-Incident:
Analysis and Review: Conduct a post-mortem analysis to enhance equipment security measures.
Security Measures: Implement additional security measures to prevent data exposure from lost equipment.