Business Continuity Plan for Spendology Solutions

Introduction

This plan ensures Spendology Solutions maintains critical operations during and after a DDoS attack.

Background

Spendology Solutions relies heavily on uninterrupted access to its SpendSmart application. A DDoS attack can disrupt this, potentially leading to financial losses and user dissatisfaction.

Scope

Covers the response to DDoS attacks, focusing on service continuity for the SpendSmart application and associated infrastructure.

Assumptions

- DDoS attacks may result in partial or full outages of the SpendSmart application.
- Timely mitigation and communication are crucial to minimizing damage.

Concept of Operations

Ensure essential services remain operational, protect company assets, and maintain customer trust through clear communication and rapid response.

System Description

The SpendSmart application integrates financial data, requiring high availability. The system relies on cloud infrastructure and various third-party services.

Overview of Three Phases

1. **Prevention**: Proactive monitoring and traffic analysis to detect potential attacks early.
2. **Mitigation**: Use of traffic filtering, rate-limiting, and coordination with ISPs to deflect malicious traffic.
3. **Recovery**: Restoring full service while ensuring minimal disruption.

Roles and Responsibilities

Task	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Traffic Monitoring & Detection	IT Security	CISO	Network Team	Management, Communications
Initial Mitigation	IT Security	IT Security Lead	ISP, Cloud Providers	Management
Communication with ISPs	IT Security	IT Security Lead	ISP	Management
Internal Stakeholder Notification	Communications Team	Management	IT Security	All Staff
Customer Notification	Communications Team	Communications Lead	IT Security	Customers
Recovery and Scaling Systems	IT Security	IT Security Lead	Cloud Providers	Management, Staff
Post-Incident Review	IT Security	CISO	All Teams Involved	Management

Activation and Notification

Activation Criteria and Procedure

- **Criteria**: System alerts indicate unusually high traffic or service outages.
- **Procedure**: Immediately notify IT Security to investigate and initiate mitigation protocols.

Notification

Internal teams, ISPs, and affected customers are notified about the ongoing attack and expected service delays.

Outage Assessment

Assess the scale and impact of the attack to determine which services are affected and prioritize recovery efforts.

Recovery

Sequence of Recovery Activities

4. Implement traffic filtering or scrubbing through a third-party provider.
5. Scale infrastructure to handle increased traffic (e.g., cloud auto-scaling).
6. Coordinate with ISPs to block attack vectors.

Recovery Procedures

- Monitor incoming traffic and apply rate-limiting or geo-blocking if necessary.
- Engage third-party DDoS protection services like Cloudflare or AWS Shield.

Recovery Escalation Notices/Awareness

Escalate to third-party vendors or external DDoS mitigation services if internal efforts are insufficient.

Reconstitution

Concurrent Processing

Once normal traffic patterns are restored, re-enable services that were disabled during the attack.

Validation Data Testing

Verify data integrity and system functionality after the attack is mitigated.

Validation Functionality Testing

Test all application functions to ensure complete recovery.

Recovery Declaration

Declare the system fully operational after confirming that all services are back online and functioning as expected.

Notification (Users)

Send out final notifications to customers regarding the recovery status, including details of any ongoing monitoring.

Cleanup

Document all steps taken during the attack response for future reference and lessons learned.

Offsite Data Storage

Ensure that all critical data is backed up offsite and is not affected by the attack.

Data Backup

Routine data backups are in place, and integrity checks are performed after any incident.

Event Documentation

Document the entire incident, including the attack's timeline, response actions, and lessons learned.

Deactivation

Stand down the response team and restore normal operations after the threat has been neutralized and full functionality confirmed.

Appendix A: Contact Information

- **ISP (e.g., Comcast, AT&T):**
- **Cloud DDoS Mitigation Provider (e.g., AWS Shield):**
- **Internal IT Security Lead:**

Appendix B: Traffic Analysis Tools and Methods

- **Tools**:
    - **Wireshark**: For packet-level traffic inspection.
    - **Cloudflare Traffic Insights**: To monitor traffic anomalies.
    - **AWS CloudWatch**: For identifying unusual traffic spikes.

- **Methods**:
    - Real-time traffic monitoring.
    - Signature-based detection for common DDoS attack patterns.
    - Geo-blocking and rate-limiting for suspicious traffic.

Appendix C: Escalation Procedures

- **Criteria for Escalation**:
    - When internal mitigation fails to reduce attack impact.
    - If attack lasts more than 30 minutes.
    - If customer-facing services are disrupted.
- **Steps for Escalation**:
    - Notify CISO and initiate cloud-based DDoS protection.
    - Contact third-party mitigation provider (e.g., Cloudflare or AWS Shield).
    - Keep internal stakeholders updated on recovery status.

Appendix D: Communication Templates

- **Internal Notification**:
    - Subject: "DDoS Attack Detected - Response in Progress"
    - Message: "A DDoS attack has been detected. IT Security is actively mitigating the attack. We will keep you informed as the situation progresses."
- **Customer Notification**:
    - Subject: "Service Disruption - Ongoing DDoS Mitigation"
    - Message: "We are currently experiencing a DDoS attack, which may affect your access to SpendSmart. Our team is working to mitigate the issue. We appreciate your patience."