Business Continuity Plan

Prepared by: Isabelle Jaber

Date: September 9th, 2024

Table of Contents:

INTRODUCTION

BACKGROUND

SPENDOLOGY SOLUTIONS is a fintech company focused on digital budgeting and financial management. As the company manages sensitive financial data through its SpendSmart application, ensuring the security and availability of its information systems is critical. A key threat to the business's continuity is a Distributed Denial of Service (DDoS) attack, which could disrupt user access to the budgeting app, compromise user trust and their overall reputation, and result in financial losses. This plan details steps to ensure minimal disruption to operations.

SCOPE

This plan covers the security of the SpendSmart application and its underlying infrastructure, including database management, user authentication, and external data integration. It applies to all technical staff responsible for maintaining the security and availability of SpendSmart, focusing on DDoS attacks and ensuring uninterrupted services.

ASSUMPTIONS

- Critical systems are monitored 24/7 for unusual traffic patterns or abnormal behavior.
- Multi-factor authentication (MFA) and encryption protocols are enforced across all systems.
- Spendology's data integration from external sources (e.g., credit card and utility companies) is secure and adheres to token-based authentication mechanisms.

CONCEPT OF OPERATIONS

SYSTEM DESCRIPTION

The SpendSmart application integrates data from credit cards and utilities companies to help users manage their finances. The system relies on cloud infrastructure and secure APIs for external data exchange. Given its sensitive nature, it is vulnerable to DDoS attacks that could overwhelm network resources, causing service outages or degraded performance.

OVERVIEW OF THREE PHASES

- **Prevention:** Implement ransomware detection tools, regular software patching, and employee training.
- **Response:** Immediate actions to minimize damage, contain the disruption, and prevent the incident from worsening. The goal is to stabilize the situation and protect the organization's critical assets.
- **Recovery:** Restore data from backups, clean infected systems, and resume normal operations.

ROLES AND RESPONSIBILITIES

		Responsible	**A**ccountable	**C**onsulted	**I**nformed
Tasks	Manages cloud infrastructure, scaling, and traffic routing.	Cloud Operations Team	Network Infrastructure Team	IT Security Team	CISO
	Monitors traffic and triggers mitigation protocols during a DDoS event	Security Operations Center (SOC) Team	IT Security Team	CISO	Board of Directors
	Supports application recovery and database troubleshooting	Development Team	IT Security Team	CISO	Board of Directors
	Ensures that post-attack recovery adheres to financial regulations and data protection standards	Compliance Team	Governance, Risk, and Compliance Team	Legal	CISO

ACTIVATION AND NOTIFICATION

ACTIVATION CRITERIA AND PROCEDURE

DETECTION

The plan is activated when abnormal traffic patterns are detected on the SpendSmart app, significantly affecting performance or access.

IMPACT ON OPERATIONS

When a disruption to critical services, systems, or processes is detected. This includes:

- Digital resources are inaccessible.
- Network outages affecting communication or access to SpendSmart or any other SPENDOLOGY SOLUTIONS resources.

LEGAL OR COMPLIANCE CONSIDERATIONS

If Sensitive Personally Identifiable Information (SPII) is compromised this triggers ethical, legal, and regulatory implications.

ACTIVATION PROCEDURE

Detect:

1. The SOC Team will monitor systems to detect traffic exceeding the normal threshold.
2. If abnormal network traffic is detected, the SOC Team will immediately notify the Computer Security Incident Response Team (CSIRT) and activate DDoS mitigation tools.

Assess:

1. The CSIRT will assess the nature, scope, and potential impact of the event according to the appropriate Incident Response Plan.
2. Based on the incident's severity classification, the Chief Information Security Officer (CISO) will activate the BCP.

Communicate:

1. The Incident Handler and communications expert will notify executive leadership, including the managing partners and legal compliance officers, of the situation.

2. A decision to declare an official business continuity event will be made, invoking the activation of the BCP.

NOTIFICATION

INTERNAL NOTIFICATION: STAFF

- Once the BCP is activated, all employees will be notified through multiple communication channels (email, phone, messaging apps) with the following information:
    - The incident type (in this case, DDoS) and the operations implications.
    - Immediate actions are required (refrain from accessing specific systems, etc).
    - Status of ongoing legal and client work.

INTERNAL NOTIFICATION: DEPARTMENTAL

- Notify IT Security, Cloud Operations, and Executive Management upon detection of the attack.
- Critical departments (IT, Legal, Finance) will receive targeted instructions for mitigating risks**,** maintaining operational continuity, and protecting client data**.**

EXTERNAL NOTIFICATION: CLIENTS

- If a breach affects client confidentiality, clients must be notified immediately as per ethical and legal obligations.
- Notify SpendSmart users of a potential outage through in-app messages (if available) and emails.
- The notification will include details about the event, the actions being taken to resolve any outage or performance issues, and any further steps clients should take.

EXTERNAL NOTIFICATION: THIRD-PARTY VENDORS

Send real-time updates to external vendors and partners who may be impacted (e.g., credit card companies, utility companies).

EXTERNAL NOTIFICATION: REGULATORY AGENCIES

If it is determined that sensitive data was put at risk during the DDoS attack, relevant law enforcement and regulatory agencies must be notified of the attack and any potential compromise to sensitive data.

EXTERNAL NOTIFICATION: CYBER INSURANCE PROVIDERS

Notify cyber insurance companies to assess coverage and begin claims processing.

COMMUNICATION METHODS

- Secure channels (encrypted emails, VPN connections) should be used to communicate sensitive information.
- For public relations, the communication team should be prepared to release a public statement outlining the firm's response to the incident without disclosing sensitive details.

OUTAGE ASSESSMENT

INITIAL ASSESSMENT

- Within the first hour of activation, the CSIRT will work with IT and other key departments to assess the scope of the outage, including:
    - Assess the impact on key services, such as user authentication, data integration from external sources, and budgeting features.
    - Evaluate if sensitive data (credit card statements, user data) is at risk during the attack.
    - Whether backups or contingency systems can be leveraged for recovery.
    - Impact on ongoing operations.

DAMAGE CLASSIFICATION

Category	Scope
Critical	Widespread disruption affecting critical servers and confirmed data loss, stolen data, unauthorized data access. This will require immediate communication with clients and regulatory bodies.
High	Major disruption, with potential data loss and significant business interruptions. This will require immediate communication with clients and regulatory bodies.

Medium	Affecting one or more critical business units (e.g., client management systems or document repositories), but alternatives or backups are available.
Low	Localized to a small number of systems or users; operations can continue with minor adjustments.

BUSINESS IMPACT ANALYSIS (BIA)

- A BIA will be conducted to identify the potential long-term effects of the outage on legal work, financial stability, and reputational risk. This involves:
    - Identifying critical processes that need to be restored first (e.g., user authentication, data integration from external sources, and budgeting features).
    - Estimating recovery times for various systems based on backup integrity and available resources.
    - Analyzing how quickly SPENDOLOGY SOLUTIONS can resume normal operations while maintaining compliance with legal and ethical obligations.

CONTINUOUS MONITORING

- Throughout the outage, the SOC Team will monitor for signs of lateral movement or further attempts by attackers to affect other systems or exfiltrate data.
- Real-time updates will be provided to the CISO to adjust the response as necessary.

RECOVERY STRATEGY

- Prioritize restoring the availability of critical IT infrastructure and restore access to client facing resources.
- Utilize a cloud-based backup/redundant system, to divert legitimate network traffic to maintain as much availability as possible and restore operations incrementally.

RECOVERY

SEQUENCE OF RECOVERY ACTIVITIES

1. **Traffic filtering:** Block malicious traffic using DDoS mitigation services.
2. **Rerouting legitimate traffic:** Use cloud-based infrastructure to route legitimate traffic away from overwhelmed systems.
3. **Notify Affected Parties**: Provide continuous updates to internal teams and clients on recovery progress.
4. **Test Restored Systems**: Validate the functionality and integrity of the restored systems before going live.
5. **Service restoration:** Gradually restore access to essential components (user login, budgeting features, databases, etc).

RECOVERY PROCEDURES

- Initiate cloud-based scaling to handle increased traffic loads.
- Implement rate-limiting to control traffic flow to critical parts of the system, such as the database storing user transactions and credit card statements.
- Prioritize restoration of sensitive user data services like encrypted database access.
- Record the incident in detail, including affected systems, timeline, actions taken, and the recovery process for legal and compliance review.

RECOVERY ESCALATION NOTICES/AWARENESS

- Executive Notifications:
    - Keep senior leadership updated on recovery progress at predefined intervals (e.g., every 4 hours).
- Client Updates:
    - Maintain transparency with clients by issuing regular updates, especially if their data is compromised.
- Legal and Compliance:
    - Provide real-time updates to legal and compliance teams to ensure that all recovery actions are within the scope of regulatory obligations. If traffic filtering fails or sensitive data is compromised, escalate the incident to the compliance and legal teams.
- Stakeholder Communication:
    - Notify external stakeholders (credit card companies, utilities) about service interruptions affecting data integration. Once critical systems are restored, issue a

formal notification to all internal and external stakeholders about the recovery completion and mitigation efforts.

RECONSTITUTION

CONCURRENT PROCESSING

Continue processing financial transactions and budgeting calculations using cloud-based backup/redundant infrastructures while primary systems are being restored.

VALIDATION DATA TESTING

- Ensure that the AES-256 encrypted sensitive financial data stored in databases remains intact and uncompromised.
- Verify the integrity of data from external sources (e.g., credit card statements) following system restoration.
- Conduct a checksum validation of critical files.
- Compare backup data with current versions to detect any discrepancies.

VALIDATION FUNCTIONALITY TESTING

- Test critical functionalities such as token-based authentication for data integration and user login through multi-factor authentication (MFA).
- Ensure secure transaction logging of user activities and financial data.
- Test data retrieval and update speed.
- Verify access controls and user permissions for all employees.

RECOVERY DECLARATION

Once SpendSmart's services are restored and performance is stabilized, the executive team will declare recovery from the DDoS event.

NOTIFICATION (USERS)

Send a notification to users via in-app messages and email that services are fully restored and secure.

CLEANUP

- Remove any temporary blocks or rerouted traffic rules.
- Review and adjust firewall and DDoS prevention rules to prevent future occurrences.

OFFSITE DATA STORAGE

- Ensure all encrypted backups of sensitive financial data are up to date and securely stored offsite.
- Maintain a regular offsite backup schedule (e.g., daily/weekly depending on case volume).
- Ensure data is encrypted and stored securely in a geographically distant location.
- Validate the availability of offsite data during monthly tests.

DATA BACKUP

- Perform a complete backup of all databases, ensuring the security of transaction logs, user data, and financial records.
- Employ both on-premises and cloud-based backup solutions.
- Conduct incremental backups nightly and full backups weekly.
- Monitor backup integrity with automated validation checks after each backup cycle.

EVENT DOCUMENTATION

- Document all details of the DDoS attack, the systems affected, and the recovery process for audit and improvement purposes.
- Submit the incident report to the legal and compliance team to ensure adherence to financial regulations within 48 hours of recovery procedure being completed.

DEACTIVATION

- The BCP will be deactivated once the system is secure, all services are restored, and the incident documentation is completed.
- Conduct a final assessment of the IT infrastructure’s availability and functionality and confirm user access.
- Deactivate temporary processes or systems initiated during the recovery period.
- Notify the C-Suite and all users of the return to normal operations.
- Conduct a post-recovery meeting to identify lessons learned and potential improvements for future responses.

APPENDICES

Appendix A: Contact Information for Key Personnel
Appendix B: DDoS Mitigation Tools and Cloud-Based Scalability Resources
Appendix C: SpendSmart Architecture Diagrams
Appendix D: Incident Response Templates for DDoS Events
Appendix E: Regulatory and Compliance Guidelines
Appendix F: Testing and Simulation Procedures for DDoS Scenarios