Fast Capital Markets Limited

POLICY DEFINING ROLES & RESPONSIBILITIES AND PLAN OF ACTION IN ORDER TO DEAL WITH DOS/DDOS ATTACKS

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31.12.2023
Policy Approved by	Board of Directors
Policy approved on	04.01.2024

Version - 1.0

Purpose and Scope

This DDoS Attack Response Policy outlines the procedures, roles, and responsibilities, along with a plan of action to mitigate and respond to Distributed Denial of Service (DDoS) attacks against our company. The objective is to ensure the availability, integrity, and security of our systems during and after an attack.

Roles and Responsibilities

Incident Response Team

- Incident Response Manager: Appointed individual responsible for overseeing the response to DDoS attacks.
- Incident Response Team (IRT): A team of cybersecurity experts responsible for implementing the DDoS response plan.

IT Operations

- Network Administrators: Responsible for monitoring and analyzing network traffic during an attack.
- System Administrators: Tasked with securing and optimizing server performance during and after an attack.

Communication Team

- Public Relations (PR): Manages external communication to clients, stakeholders, and the public.
- Internal Communication: Coordinates internal communication among teams and management.

DDoS Attack Response Plan

Detection and Identification

- Implement monitoring tools to detect abnormal traffic patterns and identify potential DDoS attacks.
- Collaborate with Internet Service Providers (ISPs) to identify and confirm DDoS attacks.

Activation of Incident Response Team

Once a DDoS attack is confirmed, the Incident Response Manager activates the Incident Response Team.

Traffic Diversion and Filtering

- Initiate traffic diversion through DDoS protection services or Content Delivery Networks (CDNs).
- Apply traffic filtering mechanisms to mitigate the impact of the attack.

System and Network Monitoring

Intensify monitoring of system and network performance to detect anomalies and assess the effectiveness of mitigation measures.

Communication Plan

Activate the communication team to inform clients, stakeholders, and the public about the ongoing situation, impact, and resolution efforts.

Collaboration with ISPs

- Collaborate with ISPs to implement network-level filtering and blocking of malicious traffic.
- Share attack information with law enforcement agencies if required.

Incident Documentation

Document all aspects of the DDoS attack, including the attack vector, duration, impact, and response actions taken.

Recovery and Post-Incident Analysis

System Recovery

- Gradually restore normal services once the attack has been mitigated.
- Conduct thorough testing to ensure the integrity and security of restored services.

Post-Incident Analysis

- Conduct a comprehensive analysis of the DDoS attack, identifying vulnerabilities and areas for improvement.
- Document lessons learned and update the DDoS response plan accordingly.

Legal and Regulatory Compliance

- Ensure compliance with legal and regulatory requirements related to reporting and managing cybersecurity incidents.
- Engage legal counsel to provide guidance on compliance matters.

Training and Awareness

Conduct regular training sessions to educate staff about DDoS threats, prevention measures, and response protocols.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff / Employees /and Directors of the Company.

Fast Capital Markets Ltd

FAST CAPITAL MARKETS LTD
KOLKATA

Binay Kumar Agarwal
Designated Officer