MCX Circular no.: MCXCCL/TECH/286/2025 December 18, 2025
MCXCCL Circular no.: MCX/MCXCCL/646/2025

Cyber Security Advisory – Learning from Incidents

In addition to previous Cyber advisories issued by the Exchange including Circular no. MCX/MCXCCL/377/2025, MCXCCL/TECH/158/2025 dated July 30, 2025, Members of the Exchange are notified as under:

The global financial services sector, including financial markets remains a prime target for sophisticated cyber threat actors. Modern cyber-attack may not be a single event, but a methodical, multi-stage operation designed for persistence and maximum impact.

The global and domestic incidents specifically targeting the BFSI sector have underscored the heightened risk faced by all market participants. Members of the Exchange have also reported few cyber incidents recently which are cited below:

- Ransomware: Ransomware Attacks have resulted in the encryption and lockdown of critical systems, leading to operational downtime, data loss, and significant financial demands.

- Phishing & Spear-Phishing: Social engineering remains the most successful entry point, often leading to credential theft and subsequent unauthorized system access.

- Data Exfiltration: Threat actors are increasingly focused on stealing sensitive customer and proprietary data for intellectual property theft or sale on the dark web, resulting in regulatory fines and loss of client trust.

- Distributed Denial of Service (DDoS): Large-scale DDoS attacks threaten to disrupt trading services and market connectivity, causing operational outages and severe economic impact.

Members are advised to review and implement the following security controls across their entire infrastructure support units to maintain a high level of readiness for any cyber events/incidents:

A. Access Control and Authentication

- Multi-Factor Authentication (MFA): Implement mandatory MFA for all remote access, sensitive applications, cloud services, and privileged accounts.

- Principle of Least Privilege (PoLP): Ensure users and service accounts are granted only the minimum access necessary to perform their specific job functions.

- Regular Audit: Conduct quarterly audits of all user accounts and access permissions, immediately disabling accounts for ex-employees or non-operational purposes.

B. Patch Management and Vulnerability

- Vulnerability Management: Implement a rigorous process for timely patching of all operating systems, applications, and network devices, prioritizing internet-facing systems and those with known vulnerabilities.

- Asset Inventory: Maintain an up-to-date and accurate inventory of all hardware and software assets.

C. Ransomware and Data Exfiltration Prevention

- Data Backup Strategy: Define data backup policy for the organisation and implement the best backups practices aligning with regulatory requirements.

- Data Loss Prevention (DLP): Deploy DLP solutions to monitor and block the unauthorized transfer of sensitive data (client IDs, financial records) outside the network.

- Endpoint/Extended Detection and Response (EDR/XDR): Replace traditional Antivirus with advanced EDR/XDR solutions to detect and isolate suspicious activity on endpoints in real-time.

D. Network Security and DDoS Mitigation

- Network Segmentation: Segment the network to isolate critical systems (Trading, Settlement) from less secure areas (e.g., general office network).

- DDoS Protection: Subscribe to and maintain a robust cloud-based DDoS mitigation service to filter malicious traffic before it impacts trading infrastructure.

E. Incident Response and Reporting

- Incident Response Plan (IRP): Maintain a tested and up-to-date IRP that clearly defines roles, communication protocols, and escalation paths for a cyber incident.

- Mandatory Reporting: Immediately report any suspected or actual cyber incident, including successful phishing or malware infections, to the Exchange and the relevant national regulatory body as per guidelines.

Cyber resilience is a shared responsibility. We urge all Members to treat this advisory with the highest priority. Non-compliance with robust cyber security standards not only puts your organisation at risk but jeopardizes the trust and stability of the entire market.

Members are requested to take note of the same.

For and on behalf of Multi Commodity Exchange Clearing Corporation Limited.

Mihir Malode
MCXCCL CISO & DPO

Kindly contact Customer Service Team on 022 68646000/ 022 50956000 or send an email at customersupport@mcxindia.com for any clarification.

---------- Corporate office ----------

Multi Commodity Exchange Clearing Corporation Limited

Exchange Square, CTS No. 255, Suren Road, Andheri (East), Mumbai – 400 093
Tel.: 022 – 6864 6000/022 - 50956000 Fax: 022 – 6649 4151 CIN: U74999MH2008PLC185349
www.mcxccl.com email: customersupport@mcxindia.com