Circular no.: MCX/TECH/367/2025 July 28, 2025

Cyber Security Advisory – July 2025

In addition to previous Cyber advisories issued by Exchange including Circular no. MCX/TECH/242/2025 dated 8th May 2025, Members of the Exchange are notified as under:

To strengthen the organization's cyber defence posture and in line with regulatory advisories (e.g., SEBI, Cert-In, NCIIPC etc.) Members advised to implement following directives, across all business and support unit to maintain a high level of readiness for any cyber events/ incidents.

- **Comprehensive asset inventory and classification of Critical/ Non-critical systems:**
  - Maintain a complete, accurate, and up-to date inventory with proper classification (Critical / Non-Critical)
  - Ensure that all IT and OT assets are inventoried, classified and tracked in a centralized asset management system. Regular audits must validate asset coverage and their respective status.

- **Vulnerability Assessment & Penetration Testing (VAPT):**
  - Conduct Vulnerability Assessment and Penetration Testing (VA/PT) at defined intervals for all internal, external, cloud- hosted, and third-party integrated assets. Critical Vulnerabilities must be remediated within defined SLAs.
  - High-severity vulnerabilities due to unpatched systems should be checked for non-compliance against patch management timelines. Other findings to be validated against VAPT closure timelines as per SEBI CSCRF guidelines, with a graded approach for closure.

- **Patch Management:**
  - Patches should be tested in non-production environment before deploying them to production environment.
  - In case of application/ system(s) from cloud services provider, the roles of Cloud Service Provider (CSP) and RE in resolving vulnerabilities and applying patches must be clearly defined in the contract.

- **Software Bill of Materials (SBOM):**
  - SBOMs must be obtained for all critical software, documenting components, dependencies, and data relationships.
  - In case the SBOM cannot be obtained for the legacy or proprietary systems, the Board/ Partners/ Proprietor of the organization should approve it with appropriate justification, rationale, and risk management approach.

- **Log Management, Data Security, and other Protect Guidelines:**
  - All log sources should be identified and collected to analyse cyber posture/ incidents. Such logs may include system, application, network, database, security, Application Program Interface (API), performance, audit trail, event and other relevant logs.

- **Threat Intelligence:**
  - Internal threat hunting must be carried out alongside threat intelligence/ advisories from sources such as NCIIPC and CERT-In etc.

- **Internet Usage & Shared Resource Access:**
  - Ensure that Shared drives and internal systems must not be accessed externally without secure VPN and MFA. Web access must be controlled via proxies and URL filtering.
  - Unrestricted internet access should be prohibited. Internet access must be role based, logged and supported with business justification in case of exceptions.

- **USB & Removable Media Controls:**
  - USB ports shall be disabled by default across all systems and any exceptions must be approved at the highest level within the organisation.
  - Strengthen effectiveness of existing security controls and incident management plan.

- **DC-DR Drills**
  - Scenario-based cybersecurity drills as specified in SEBI CSCRF (*Annexure-E*) should be conducted periodically to test incident response and recovery capabilities.

Members are requested to take note of the same.

For and on behalf of
Multi Commodity Exchange of India Ltd.

Sougat Ghosh
CISO & DPO – MCX

Kindly contact Customer Support on 022 - 6649 4040 or send an email at customersupport@mcxindia.com for further clarification.