

Department : Cyber and Information Security

Download Ref No: NCL/CIS/45748

Date : September 18, 2020

Circular Ref. No: 02/2020

All Members,

Sub: Cyber Security Advisory - Prevention of DDoS Cyber attacks and Cyber Security preparedness

It has been observed that during lockdown period there were drastic increase in cyber-attacks on BFSI sector especially on institutes rendering financial services. Recently, operations of one of the stock exchange in Asia Pacific region were disrupted continuously by DDoS cyber-attack.

In order to ensure continuous availability of services and prevent cyber-attacks, all members/participants are requested to ensure the following:

1. Review cyber security safeguards put in place for protecting the business operations and fix the identified gaps on priority.
2. Review security of communication links like MPLS lines, point to point leased lines, Internet leased lines etc. provisioned for trading, communications and other services exposed to the customers and partners on the internet/private networks.
3. Ensure all the internet links and services are adequately protected from cyber-attacks including DoS/DDoS attacks.
4. Ensure enough safeguards are put in place to protect private networks from man in the middle type of attacks and shall use end to end encryption for communication channels/protocols.
5. Ensure adequate redundancy and high availability for private networks provisioned for business operations availing services from multiple service providers.
6. Review vulnerabilities of business applications and ensure enough safeguards for targeted application attacks.
7. If employees/outsourced staff managing business operations are working from home, ensure adequate safety and security measures (such as hardening of employees home PCs/laptops, ensuring licensed version of anti-virus, secure VPN access with 2 FA etc.) before providing access to corporate network/office systems.
8. Continuously monitor applications and services for their availability and good response time.

Members / participants are requested to adhere to the cyber security guidelines / advisories issued by SEBI, CERT-In, NCIIPC and follow best industry practices and comply with other guidelines issued from time to time and ensure that utmost importance is given to the cyber security preparedness and in case of any cyber security breach/incident/deficiency, reporting shall be done as per the Standard Operating Procedure for reporting of cyber security breaches, incidents and deficiencies.

For and on behalf of

**Chief Information Security Officer
NSE Clearing**

Telephone No	Fax No	Email id
022-26598100 Ext. 20002	022-26598120	cdc@nse.co.in