MCX
METAL & ENERGY
Trade with Trust

Circular No.: MCX/TECH/800/2020 October 27, 2020

Cyber Security Advisory – Remote access and Telecommuting

In terms of provisions of the Rules, Bye-Laws and Business Rules of the Exchange Members of the Exchange are hereby notified as under:

Due to Covid-19 pandemic market participants have started work from home facility. In the current situation work from home is new normal and due to the remote access and telecommuting attracting cyber-threats. Members are therefore requested to implement the following measures as stipulated by the SEBI;

1. The members shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.
2. For implementation of the concept of trusted machine as end users, the member shall categorize the machines as official desktops / laptops and accordingly the same may be configured to ensure implementation of solution stack considering the requirements of authorized access. Official devices shall have appropriate security measures to ensure that the configuration is not tampered with. The member shall ensure that internet connectivity provided on all official devices shall not be used for any purpose other than the use of remote access to data centre resources.
3. If personal devices (BYOD) are allowed for general functions, then appropriate guidelines should be issued to indicate positive and negative list of applications that are permitted on such devices. Further, these devices should be subject to periodic audit.
4. The member shall implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.
5. The member shall ensure that the trusted machine is the only client permitted to access the data centre resources. The member shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.
6. The member shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. The member shall implement short session timeouts for better security. Towards this end, it is suggested that the member may consider running a mandatory monitor on the device that executes:
   a) At random intervals takes a picture with the webcam and uploads the same to the member's server,

   b) At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the member server as a security event.

7. The member shall ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for service providers.
8. Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the member shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.
9. The member shall ensure that the backup, restore and archival functions work seamlessly, particularly if the users have been provided remote access to internal systems.
10. The member is advised to exercise sound judgement and discretion while applying patches to existing hardware and software and apply only those patches which were necessary and applicable.
11. The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.
12. The member shall update its incidence response plan in view of the current pandemic.
13. The member shall implement cyber security advisories received from SEBI, MII, CERT-IN and NCIIPC on a regular basis.
14. Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness.

Exchange is also in process to collect the feedback from the members on the above advisories as required by the SEBI. Exchange shall inform to the members about the process of submission of the feedback through separate circular.

Members are requested to ensure safety of their organization and employees by keeping a close watch on their IT infrastructure for timely detection and prevention to any such Cyber-attacks.

All Members and their constituents are requested to take note of the above and take necessary steps on immediate basis.

Jagdish Asodekar
CISO