All Segment

April 17, 2020

Circular No. : MCCIL/IT/1623/2020

Sub: Cyber Security Advisory in view of Covid-19 Pandemic and resultant Lockdown

In terms of the provisions of the Rules, Bye-Laws and Regulations of the Metropolitan Clearing Corporation of India Limited (MCCIL), Clearing Members of the MCCIL are notified as under:

There are news reports that cyber criminals around the world are capitalizing on the Covid-19 crisis by exploiting the remote working vulnerabilities on computers, routers and unprotected home networks. A cyber attack on critical devices, data or network links may be devastating and cause infrastructure failures. Hence it is advised that we should be vigilant and follow the Cyber Security Guidelines issued by SEBI and the best practices and advisories issued by the CERT and NCIIPC, as given in the **Annexure.**

Members are requested to ensure safety by keeping a close watch on their IT infrastructure for timely detection and prevention of cyber attacks. For clarifications, members may contact Customer Service on 022-61129010 or send an email to **info@mclear.in**

Sec_rity is incomplete without U!

For and on behalf of
Metropolitan Clearing Corporation of India Limited

Sumit Badakh

Head Information Technology

Annexure

Below are some of the attack vectors and vulnerabilities targeted by Cyber Criminals:

1. Exploitation of Virtual Private Network (VPN) and Remote Desktop Connectivity Vulnerabilities

Remote Login Attacks: Remote User Credential Theft, which could result in financial and reputational damage to the organizations.

2. Malware Attacks:

a. Users working with home systems for official work could fall for “free” access to obscure websites or pirated shows, opening the door to likely malware and attacks.

b. Viruses, malware campaigns and ransomware such as TrickBot, Emotet, NanoCore, Crimson RAT etc. are increasingly seen being used by cybercriminals during this period.

3. Social Engineering Attacks such as Phishing:

a. Phishing emails with links claiming to have important updates on Coronavirus from World Health Organization (WHO), Coronavirus Maps, Promotional Codes. The links, if clicked may lead the devices being infected with malware/ransomware.

b. Malicious / Fraudulent websites and URLS.

Below are some of the best practices and recommendations, which should be followed by the Organizations:

1. Ensure all Systems are protected with appropriately configured firewalls policies.

2. Monitor and assess remote access solutions for their capacity to make adequate provisions as per assessment.

3. Ensure Remote Access to the organization's network is access strictly through secured connectivity like VPN using multi-factor authentication.

4. Secure all systems that enable remote access through VPN are fully patched and have anti-malware/anti-intrusion prevention with latest signatures.

5. Enforcement of strict application whitelisting, blocking unused ports, turning off unused services and monitoring outgoing traffic are some of the measures to prevent cyber-attacks from occurring.

6. Ensure systems are equipped to Monitor, block and trigger alerts for any abnormal activity/behavior related to - Network traffic, Internet-facing applications, all Ports and critical processes.

7. Network segmentation and access right differentiation are both required. It is recommended that even remote user activity is covered by the organization's perimeter security tools.

8. Check the availability and duration of logging remote user actions. Ensure that remote sessions automatically time out after a specified period of inactivity and that they require re-authentication to gain access.

9. Remind employees of the types of information that they need to safeguard. This often includes information such as confidential business information, trade secrets, protected intellectual property and other personal information.

10. Majority of the cyber-attacks are primarily introduced via phishing emails, malicious messages through websites and social media and malicious apps. Hence, it is critical to advise employees / vendor staff to not to click links and attachments which are suspicious and to check all mails and messages for authentic URLs, domain names and spelling errors.

11. Do not allow sharing of work computers and other devices. When employees bring work devices home, those devices should not be shared with or used by anyone else in the home. This reduces the risk of unauthorized or inadvertent access to protected company information.

12. "Remember password" functions should always be turned off when employees are logging into company information systems and applications from their personal devices.

13. Consider Mobile Device Management (MDM) and Mobile Application Management (MAM). These tools can allow organizations to remotely implement a number of security measures, including data encryption, malware scans, and wiping data on stolen devices.

14. Employees and support staff must be made aware on IT and Cyber Security support mechanisms.

15. Employees and related vendor staff should be educated about incident reporting mechanisms in the organization.

16. Deploy anti-spam solutions and update spam block lists on timely basis.

Below are some of the best practices and recommendations, which should be followed by the Employees/ Support/Vendor Staff while remote working/ working from home:

1. Change default passwords on your home Wi-Fi router to prevent hackers accessing your network.

2. Ensure home devices are updated with latest security patches of OS, antivirus and malware protection software.

3. Use strong and unique passwords on every account and device.

4. Only use software your company would typically use to share files. Refrain from using your personal email or 3rd party services unless reliably informed otherwise.

5. Avoid accessing the corporate network through third-party services that use intermediate servers and take over the responsibility for authorization and authentication issues.

6. When signing for any new services, verify the source of every URL and ensure the program or applications installed are the original versions from a trusted source.

7. Always ensure protection of your organizational and customer data.

8. Always exercise caution while opening emails from unknown senders and the attachments in such emails.