Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2020-0008

Cyber security during covid-19 outbreak

Original Issue Date: March 26, 2020
Updated: March 30, 2020

Severity Rating: High

Description

Many organisations are being encouraged its staff to work from home to help stop the spread of corona virus. Switching to remote working because of the covid-19 can create cyber security problems for employers and employees.

There is an increase in the number of cyber attacks on computers, routers and unprotected home networks used by employees who have switched to remote working due to the spread of covid-19.

Cyber criminals are exploiting the covid-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organisations.

With most employees working from home, enterprise VPN servers have now become paramount to a company's backbone, and their security and availability must be the focus going forward for IT teams. It is important that the VPN service is patched and up-to-date because there will be way more scrutiny against these services.

Security best practices

- Change default passwords on your home Wi-Fi router to prevent hackers accessing your network
- Use strong and unique passwords on every account and device - consider using two-factor authentication (2FA).
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
- 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.
- Avoid accessing the corporate network through third-party services that use intermediate servers and take over the responsibility for authorization and authentication issues.
- 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.
- 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.
- 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.
- 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.
- "Remember password" functions should always be turned off when employees are logging into company information systems and applications from their personal devices.
- 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.

References

Practical steps to work from home Securely
https://workfromhome.globalcyberalliance.org

Work from home - Best practices
https://www.dsci.in/sites/default/files/DSCI-WorkfromHomeAdvisory-1.pdf

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India