Guidelines to Improve Cyber Security to Enable Work from Home.

ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
Presidential Secretariat

SRI LANKA CERT|CC

Minimal Guidelines for IT Administrators.

Issued: 10th December, 2020

The following are the minimum set of guidelines an IT administrator must adapt to secure your infrastructure when enabling working from home at your organization. You must put in place an appropriate cyber security strategy depending on your organization's security requirements and comply with government cyber security guidelines published from time to time.

Remote Access

- Facilitate a secure remote access system (ex: SSL VPN, VDI etc.) for the end users to connect to the office network.
- Setup appropriate idle time to terminate inactive remote sessions.
- Maintain an inventory of remote access user accounts and review them periodically. Remove or disable remote access users who no longer require access or have left the organization.
- All Endpoints including devices used for remote access should be adequately protected (up to date patching OS & Antivirus signatures).
- Deploy Anti-Virus/EDR solutions with features like ransomware protection, anti-spam, web protection to better secure your personal devices, networks, applications and data.

Application & Software Security

Websites & Web Application Protection

- Should be placed behind a Web Application Firewall.
- Should be installed with appropriate SSL certificate.
- Periodic web application penetration tests must be performed to identify the vulnerabilities.
- Vulnerabilities must be remediated on a timely basis.

Software & Applications

- Use genuine licensed software.
- Apply patches as and when published by the vendor.
- Restrict access to your infrastructure from countries that are not related to the operations to avoid threats.

Collaboration & Web Conferencing

- Use only management approved platforms for collaboration.
- Always keep the remote meeting software updated.
- Do not share online meeting request emails with unauthorized parties in order to avoid unknown parties joining a meeting.

Security Monitoring & Incident Management

Appropriate actions must be taken on identified Incidents.

Login Failure

- Regularly review failed logins including remote access logins and website/application logins and take action.
- Incident logs must be backed up for incident analysis.
- Regularly review suspected access from countries that are not related to the operations.

Security Alerts

- Regularly review the alerts generated by the security devices not limited to firewalls, IDS/IPS,VPN Servers and antivirus for suspected activities and take action.

Websites

- Regularly monitor website internet facing applications defacement and denial of service attack and take action.

Incident Reporting

- All staff should be made aware to report any suspicious activity to the department head and IT.
- Report any information security incident immediately to your department heads and to incidents @cert.gov.lk.

Data Security & Storage

- All information should be backed up to a location and back up frequency determined by your management.
- Refrain backing up and storing organizational information on unauthorized removable media and cloud storage.

User Awareness

- Regularly educate and make staff aware to adhere to the organization's information security policies and best practices.