Government of Telangana
Aarogyasri Health Care Trust

CIRUCLAR

Circular No. AHCT/PMU Dept.,/2017, Date: / 05/2017.

Sub: AHCT – PMU Dept., - Steps to be taken to prevent Ransomware Attack on client side computers (Network Hospitals) – Reg.

****

It is to inform that, for the last two days, ransomware(Computer Virus) has been attacking many computers all over the world. To prevent such attacks on Aarogyasri IT Application, all the network Hospitals are instructed to take following steps without fail.

Best practices to prevent ransomware attacks:

- Install Updated and Genuine Operating System in all the Computers(Windows 10)
- Maintain updated Antivirus software on all systems
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- **Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser**
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.

- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Disable remote Desktop Connections, employ least-privileged accounts.
- If not required consider disabling, PowerShell /windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta[js|wsf
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies

Chief Executive Officer

To

1. The MDs/CEOs/Medical Superintendents of all the Network Hospitals.
2. The GM (FOSS), AHCT with a request to communicate to all District Coordinators of State of Telangana.

Copy to:

1. All the HoDs, AHCT
2. The PS to CEO, AHCT for favour of information.