Guidelines for mitigating ransomware Incidents

- Users should be alerted not to open attachments in unsolicited e-mails, even if they come from people in your contact list; never click on a URL contained in an unsolicited e-mail unless you are sure it is genuine. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Block Tor, Peer to Peer (P2P) /Torrent traffic in Systems and Network.
- Application white listing/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.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsfRDP
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Ensure file share and RDP are disabled on all systems. Disable SMB service and port at network/ host firewall. Also remove team viewer, Any desk from all machines
- Remove temporary files/folders.
- Review firewall rules. Inbound connections may be blocked unless you have specific requirements. Enable outbound connections only for essential ports like http, https, email, DNS.
- Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access.
- Disable unused USB ports and USB storage device auto run;
- 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.
- 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.
- Use strong authentication protocol, such as Network Level Authentication (NLA) in Windows.
- Run updated Windows Defender, Trend Micro antivirus or other free ones like Malwarebytes, Avast, Avira

General Security Guidelines

Best practices for securing Operating system

- Keep operating system up to date with the latest service pack and patches to protect against common attacks.
- Remove all unneeded users and groups.
- Disable unwanted services and protocols.
- Configure access controls for all protected files, directories, devices.
- Restrict access of operating system source files, configuration files, and their directories to authorized administrators.
- Use Strong Password for user accounts.
- Antivirus for scanning/detecting/cleaning must be installed on the Servers/Computer system and it should be regularly updated.
- Regularly review the server log files (Access/Error/Security logs) for knowing any attacks and intrusions, preferably daily. Logs with HTTP error code 403 (Forbidden) and 404 (Not found) may be malicious attempts. Any actual incident may be reported to cert.ksitm@kerala.gov.in.
- Take regular back up of application and db.

Best practices for securing Web Server

- Install the latest version of the web server software along with the latest security patches.
- Install only the required features of the application server and remove default features not being used.
- Remove all sample files scripts, manuals and executable code from the web server application root directory.
- Remove all files that are not part of the website.
- Remove the web server banner information so that web server and operating system type and version are not reported.
- Make sure that a dedicated User account with limited privileges should be used for the Web Server Processes.
- All default user names and IIS/apache pages (like admin, default.aspx, index.aspx...etc) should be renamed.
- The configuration files of the web server process should be readable by web server process but not writable.
- Consider security implications before selecting programs, scripts and plug-ins for the webserver.
- Third party free modules available should not be used without proper checking and verification of their functionality and security.
- Use the correct CHMOD for each folder and file-Setting files or folders to a CHMOD

of 777 or 707 is only necessary when a script needs to write to that file or directory.

- Use web application firewall for monitoring/ filtering the request in order to prevent hacking attempts.

Best practices for securing Application

- Update the core application/installed plugins to the latest stable version or whenever the patches are available.
- Limit Dashboard access to administrator only or limit by specific capability. Change the default name of the login page (admin) to a customized one.
- Use Strong password: Always use strong password for the administrator accounts. An example of strong password is E@^M!$<9@k (min of 10 characters). At least every three months changing your password regularly is a healthy practice for your website's security.
- Prevent code injection - The best defense against code injection vulnerabilities is to prevent the inclusion of executable user input in code. User input used in dynamic code must be sanitized, for example, to ensure that it contains only valid, white listed characters. Sanitization is best performed immediately after the data has been input, using methods from the data abstraction used to store and process the data. Make sure that the unencrypted sensitive information is not stored on the client side.
- Prevent Arbitrary File Upload - The file types allowed to be uploaded should be restricted to only those that is necessary for the application functionality. Please ensure the following recommendations to prevent file upload vulnerability.
  - Never accept a filename and its extension directly without having a whitelist filter.
  - Ensure that files with double extensions cannot be executed.
  - Limit the filename length.
  - Rename the files that are uploaded.
  - Use randomly generated filenames for uploaded files.
  - Check for the correct MIME type of file before uploading. The application should perform filtering and content checking on any files which are uploaded to the server.
  - Make sure that the uploaded directory should not have any "execute" permission and all the script handlers should be removed from these directories.
- Disable directory listing in the web or application - server configuration by default. Restrict access to unnecessary directories and files. Create an index (default) file for each directory.
- Make sure that a custom error page is shown when trying to access unauthorized URLs in the website and when errors result rather than the webserver displaying default error page which may disclose sensitive information such as webserver technologies used, SQL queries etc.
- All Passwords, connection strings, tokens, keys…etc., should be encrypted with salted

hash. There should not be any plain passwords stored in config files or source code or in database.

- Sensitive data should always be transferred to the server over an encrypted connection. It is recommended to use TLS 1.2 or higher. Disable older protocols (like TLS 1.1, 1.0, SSLV3 etc) in the server.