CYBER SECURITY ADVISORY PREVENTION AGAINST CYBER ATTACKS ON MICROSOFT INFRASTRUCTURE (ADVISORY NO. 72)

1. **Introduction.** Microsoft products / infrastructure (**Active Directory, Servers, Cloud, intelligence & endpoints** etc) are being used for **core business operations** within public / private organizations. Organizations also invest on Cyber Security products to secure their IT infrastructure from malware / hostile attacks. A successful execution of malware on organization's network or domain controller can lead to financial loss, data stealing and widespread disruption of services. In Oct 2021, Microsoft released Digital Defense Report rendering an actionable insight into Microsoft products. Accordingly, precautions / recommendations mentioned below must be followed to secure Microsoft infrastructure within public / private organizations.

2. **Recommendations**

   a. **System / Network Administrators**

      (1) Domain controllers (AD servers) must be regularly monitored for signs of malware infection. Endpoints and network logs should be examined on regular basis to detect anomalous network traffic.

      (2) Windows commands / utilities such as **mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe** are **not required by the end-users** and **must be blacklisted for endpoint execution**.

      (3) Administrators must block execution of all scripts having .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif, .ps1 extensions.

      (4) **Block outbound network connections** from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.

      (5) Establish a **Sender Policy Framework (SPF) for domain**, which is an email validation system designed to prevent spam / malware attachments by detecting email spoofing.

      (6) **Application whitelisting** and **strict implementation of Software Restriction Polices (SRP)** be ensured to block binaries running from **%APPDATA%** and **%TEMP%** paths.

      (7) Block attachments of file types: exe, .pif, .tmp, .url, .vb, .vbe, .scr, .reg, .cer, .pst, .cmd, .com, .bat, .dll, .dat, .hta, .js and .wsf in the emails.

      (8) Block execution of above file types (para 2a(7) in Windows environment as most ransomware / trojan samples rely on free execution of these files types.

      (9) Update / patch Microsoft Windows vulnerabilities and other installed software.

(10) Disable RDP of all endpoints (when not required) and patch it against all latest vulnerabilities. **Establish site-to-site VPN for remote access / employ zero trust architecture for accessing services**.

(11) Centralized monitoring of endpoint Windows logs must be performed to detect anomalous user behavior.

(12) Regularly update antimalware solutions running on endpoints in enterprise environment as well as standalone systems

(13) Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. This data should be kept on a separate system / storage and backups should be stored offline.

(14) Protect data through backups and passwords.

(15) Apply least privileged access across network.

(16) Prioritize authentication and authorization in systems and domains.

(17) System / Network Administrators must regularly update their skills and knowledge about latest trends in cyber security.

(18) Educate endusers regarding cyber security best practices and antimalware measures.

b. **End-users**

(1) **Regularly update reputed antiviruses** such as Kaspersky, Avira, Avast etc to scan system regularly.

(2) **Do not download attachments from emails or websites unless you are sure about the source / sender**.

(3) Avoid downloading software from untrusted websites or torrents.

(4) Use Chrome / Firefox for browsing internet instead of Internet Explorer.

(5) Make sure that web browser is up-to-date and no plugins other than adblock or adblock plus is enabled.

(6) Enable multi-factor authentication on all email and banking accounts.

3. **Microsoft Digital Defense Report 2021.** Gist of actionable items from subject report has been incorporated in **Para-2**, however, for supplementary details on Microsoft infrastructure, please visit https://query.prod.cms.rt.micrsoft.com