Subject: - **Advisory – Prevention against Cyber Espionage (Advisory No. 15)**

Context. Hostile threat actors are actively targeting networks of sensitive organizations to extract critical information. Numerous malware samples have indicated that hostile elements make use of **public exploits, customized payloads** and **spear phishing** to compromise endpoints. Therefore, recommendations mentioned below must be followed.

2. **Recommendations**

a. Implement all accounts with password logins (e.g service account, admin accounts & domain accounts) to have strong & unique passwords.

b. Implement multi-factor authentication for all services to the extent possible, particularly for webmail, virtual private networks and accounts that access critical systems.

c. Use updated Operating System & Antivirus.

d. Remove unnecessary access to administrative shares.

e. Disable remote desktop connections & employ least privileged accounts.

f. Limit users who can log in using remote desktop and implement an account lockout policy.

g. Implement and verify domain-based message authentication, reporting and conformance (DMARC), Domain Keys Identified Mails (DKIM) and Sender Policy Framework (SPF).

h. Use two-factor authentication may also be considered for official email accounts.

i. Do not open attachments in unsolicited emails. Furthermore, never click on any external links.

j. Deploy firewalls and closely monitor IN/OUT traffic to observe any anomalies / attack patterns.