Circular

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Bolstering Defenses Against Increased Cyber Threats

Date: 15/06/2025

EXECUTIVE SUMMARY:

The Cybersecurity Council offer sincere appreciation for your ongoing cooperation and dedication to secure digital transformation and optimal cybersecurity practices.
Amid rising geopolitical tensions and a surge in malicious cyber operations worldwide, organizations are facing increased risks from threat actors exploiting vulnerabilities, launching phishing campaigns, and targeting critical systems. These threats can result in significant operational disruption, data theft, reputational harm, and financial loss.

RECOMMENDATIONS:

- Activate the cyber operation center and remain vigilant and promptly report any unusual or suspicious activities targeting the sectors.
- Consider anti-DDoS solutions from ISPs or security vendors, if already subscribed then verify the anti-DDoS configuration.
- Have a DDoS response plan in place to respond quickly and effectively.
- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- **Increase Vigilance and Monitoring**
  - Closely monitor for anomalies, unauthorized access attempts, and suspicious outbound traffic.
  - Enable real-time alerting and ensure around-the-clock monitoring where possible.
- **Patch and Harden Systems**
  - Apply all critical updates and security patches to operating systems, applications, and devices.
  - Prioritize known exploited vulnerabilities and internet-facing services.
- **Strengthen Identity and Access Management**
  - Enforce Multi-Factor Authentication (MFA) across all user accounts, especially for remote and privileged access.
  - Audit and restrict administrative privileges to only essential personnel.
- **Segment and Secure Critical Infrastructure**
  - Implement network segmentation and isolate sensitive systems.
  - Disable unnecessary services, ports, and remote access where not essential.
- **Review and Update Incident Response Plans**
  - Ensure clear roles, escalation procedures, and communication plans are in place.
  - Conduct tabletop exercises and verify the readiness of incident response teams.
- **Backup and Recovery Readiness**
  - Maintain encrypted, offline backups of all critical systems and data.
  - Test restoration procedures to confirm rapid recovery capability.
- **Raise Awareness and Train Staff**
  - Educate employees on phishing threats, social engineering tactics, and secure practices.
  - Encourage prompt reporting of suspicious emails or activities.

Kindly disseminate this information to your respective departments and relevant entities for their awareness and action as needed.

We appreciate your continued cooperation in ensuring cybersecurity.