مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Bolstering Defenses Against Increased Cyber Threats

Date:25-10-2024

EXECUTIVE SUMMARY:

The UAE Cybersecurity Council (CSC) appreciates your ongoing collaboration in promoting secure digital transformation and effective cybersecurity practices. In light of the recent surge in cyber-attacks targeting various sectors, the UAE Cybersecurity Council urges all entities to remain vigilant and proactive in safeguarding your digital environments. To enhance cyber resilience, the CSC strongly urges all organizations to implement the following measures immediately.

Necessary Security Measures:

- 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 cyber threat intelligence sources for information on potential threats targeting the industry.
- Ensure that all software, operating systems, and security applications are up to date with the latest patches and updates.
- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- Develop a comprehensive incident response plan that includes procedures for identifying, containing, and mitigating cyber incidents.
- Phishing Attacks: Be cautious of unsolicited emails, messages, or calls requesting personal information or financial details.
- Use Strong Passwords: Employ strong, unique passwords for each online account and enable multi-factor authentication wherever possible.
- Backup Important Data: Regularly backup critical data to secure, offline storage solutions.

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.