GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *112
TO BE ANSWERED ON: 09.02.2022

CYBER ATTACKS

***112. DR. ARVIND KUMAR SHARMA:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the Government is aware of the fact that India is one of the most cyber targeted countries in the world;

(b) if so, whether the Government is making efforts to address the above mentioned situation; and

(c) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (c): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. *112 FOR 09.02.2022 REGARDING CYBER ATTACKS

…….

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. As the internet expands and delivers many benefits for citizens, the Government is fully aware of growing instances of user harms, criminality and cyber threats online. Further, there has been media articles, citing a report published by IBM X-Force (A threat intelligence sharing platform), stating that India was the second most Cyber attacked country in Asia-Pacific in year 2020. The findings of such reports by cyber security vendors are generally based on data generated by their products and details of such data is not available and hence cannot be verified.

(b) and (c): Government is fully cognizant and aware of various cyber security threats; and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
ii. CERT-In is also operating Responsible Vulnerability Disclosure and Coordination program to encourage vulnerability identification and remediation in the country.
iii. CERT-In is operating an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
iv. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
v. All the government websites and applications are audited with respect to cyber security prior to their hosting. Auditing of the websites and applications is conducted on a regular basis after hosting also.
vi. CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.
vii. The Government has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State/UT Governments and their organizations and critical sectors.
viii. Cyber security mock drills are conducted regularly in Government and critical sectors. 64 such drills have so far been conducted by CERT-In where 820 organisations from different States and sectors participated.
ix. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

x. CERT-In is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

xi. CERT-In is providing the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to containment and mitigation of cyber security incidents reported from the financial sector.

xii. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

xiii. CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

xiv. 24x7 Security Monitoring Centre is in place at National Informatics Centre (NIC) for detecting and responding to security incidents related to NIC infrastructure and data centres. Additionally for enhancing data security, periodic security audits and vulnerability assessment of resources are performed followed by subsequent hardenings.

xv. Ministry of Home Affairs (MHA) has issued National Information Security Policy and Guidelines (NISPG) to the Central Ministries as well as the State Governments/Union Territories in order to prevent information security breaches/Cyber intrusions in ICT infrastructure.

xvi. Indian Cyber Crime Coordination Centre (I4C) under MHA has been designated as the nodal point in the fight against cybercrime. Government has launched National Cyber Crime reporting portal namely www.cybercrime.gov.in to enable public to report incidents pertaining to all types of cyber-crimes with a special focus on cyber-crimes against women and children

xvii. The analytic centre at National Critical Information Infrastructure Protection Centre (NCIIPC) provides near real time threat intelligence and situation awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure / Protected System entities to avert cyber-attacks.

****