GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2646
TO BE ANSWERED ON: 25.03.2022

PREVENTION OF CYBER ATTACKS

2646 SHRI SUJEET KUMAR:

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

(a) whether more than 11.5 lakh incidents of cyber attacks were tracked and reported to India's Computer Emergency Response Team (CERT-In) in 2021;

(b) whether power companies, oil and gas majors, telecom vendors, restaurant chains and even diagnostic labs have been the victims of cyber attacks;

(c) the steps that have been taken by the Ministry to prevent cyber security incidents and keep cyber space free from such nuisance; and

(d) whether Government has taken any steps to update its current cyber security framework amidst growing reports of cyber attacks in the country?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users.

Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported that a total number of 14,02,809 cyber security incidents are observed during the year 2021.

(b): As per CERT-In, cyber security incidents are observed across various sectors such as E-Commerce, Energy, Finance, Government, Healthcare, Information Technology, Manufacturing, Telecom, Transportation etc.

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

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 operates an automated cyber threat exchange platform for proactively collection, analysis and sharing of tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

iii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

iv. All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

v. CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. The Government has formulated a Cyber Crisis Management Plan 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.

vii. 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.

viii. CERT-In conducts regular training programmes workshops for Ministries, Departments, States & UTs and organizations to sensitise them about the cyber security threat landscape and enable them to prepare and implement the Cyber Crisis Management Plan (CCMP). 128 CCMP workshops have been conducted till February 2022 by CERT-In. Out of these, 31 CCMP workshops conducted during the year 2021.

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 operates 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 provides 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 the 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.

(d): Government has formulated a draft National Cyber Security Strategy (NCSS) which holistically looks at addressing the issues of security of national cyberspace. The vision of the Cyber Security Strategy is to "Ensure a safe, secure, trusted, resilient and vibrant cyber space for India's prosperity". NCSS is under process for approval.

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.

****