GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2019
TO BE ANSWERED ON: 17.03.2023

GROWING CYBER THREATS

2019. SHRI VIVEK K. TANKHA:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the steps being taken to prevent and build robust mechanism against cyber threats since around 2000 Indian websites were hacked in June-July 2022 alone and All India Institute of Medical Sciences (AIIMS), Delhi servers went out of order on 23rd November, 2022 and is yet to be resolved completely; and

(b) how effective has been the Indian Computer Emergency Response Team (CERT-In) in dealing with such threats and details of the response of CERT-In, incident-wise?

ANSWER

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

(a) and (b): Government is committed to ensure that Internet in India is Open, Safe and Trusted and Accountable for its users and is fully cognizant and aware of various cybersecurity threats. With emergence of new technology and rise in the usage of Internet, increase in cyber incidents is a global phenomenon.

As per section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is the national agency for coordination of cyber incident response activities. CERT-In is mandated to track and monitor cyber security incidents in India. CERT-In operates 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. The following measures have been taken to prevent and build a robust mechanism against cyber threats:

(i) CERT-In is operating a 24x7 incident response helpdesk. CERT-In has tracked, received reports regarding and handled a total of 11,58,208, 14,02,809 and 13,91,457 cybersecurity incidents during the years 2020, 2021 and 2022 respectively. Cybersecurity incidents, such as phishing, distributed denial of service attacks, website intrusions, malware infections, ransomware attacks, vulnerable services and targeted attacks were handled by CERT-In through coordinated measures within and outside the country with affected organisations, service providers, product and security companies, research institutions and academia, law enforcement agencies, international CERTs, regulators and stakeholders.

(ii) CERT-In, in December 2022, issued a special advisory on best practices to enhance the resilience of health sector entities, and has requested the Ministry of Health and Family Welfare to disseminate the same to all authorised medical care entities and service providers in the country.

(iii) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

(iv) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis. CERT-In has also published “India Ransomware Report H1 – 2022” in August 2022, covering latest tactics and techniques of ransomware attackers and ransomware specific Incident response and mitigation measures.

(v) CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats. It operates 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.

(vi) CERT-In regularly conducts training programmes for network and system administrators and chief information security officers of government and critical sector organisations, regarding securing the information technology infrastructure and mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022.

(vii) Government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to hosting.

(viii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(ix) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(x) Cyber security mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the government and the critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from various States and sectors participated.

(xi) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.

(xii) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safe Internet Day on 8.2.2022 and Cyber Security Awareness Month in October 2022 by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre of development of advance computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices etc. through videos and quizzes on MyGov platform.

(xiii) CERT-In and the Reserve Bank of India jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

****