GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2537
TO BE ANSWERED ON: 11.12.2024

RISING THREAT OF CYBER ATTACKS

2537. SHRI ADHIKARI DEEPAK DEV:

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

the manner in which the Government is addressing the rising threat of cyber-attacks and ensuring the cybersecurity crucial infrastructure, financial system and personal data?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for its users. Government is fully cognizant and aware of various cyber threats and challenges. To strengthen the nation's cybersecurity posture and ensure the protection of critical infrastructure, financial system and personal data, the Government has taken several key initiatives which, inter alia, includes:

i. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.
ii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
iii. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
iv. The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000.
v. NCIIPC provides threat intelligence, situational awareness, alerts &advisories and information on vulnerabilities to organisations having Critical Information Infrastructure (CIIs)/ Protected Systems (PSs) for taking preventive measures from cyberattacks and cyber terrorism. It also provides all cyber security related advice to these organisations, whenever asked for.
vi. The Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) has been setup for responding to and containing and mitigating cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.
vii. CERT-In operates an automated cyber threat intelligence exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
viii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

ix. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

x. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

xi. CERT-In issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

xii. CERT-In issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024 to help organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

xiii. CERT-In issued an advisory to various Ministries in November 2023 outlining the measures to be taken for strengthening the cyber security by all entities that are processing digital personal data or information including sensitive personal data or information.

xiv. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors.

xv. National Informatics Centre (NIC) provides Information Technology (IT) support to ministries, departments and agencies of the Central Government, State Governments and district administrators for various e-governance solutions and follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber attacks and safeguarding data.

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

xvii. RBI has directed all payment system operators to get Audit of their payment system done by a CERT-In empanelled auditors on an annual basis and submit the report to RBI within two months of close of their respective financial year.

xviii. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.

xix. In order to ensure data protection, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ('SPDI Rules') mandates reasonable security practices and procedures for compliant body corporate or any person on its behalf, handling sensitive personal data or information. Body corporate or any person on its behalf shall obtain written consent from the provider of such information regarding lawful purpose of usage before collection of such information.

xx. Further, in order to safeguard the personal data of individuals and ensure that their data is shared only with their consent, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted. The DPDP Act is aimed at safeguarding the personal data of individuals, including consumers in the e-commerce sector and ensuring processing of personal data for the lawful purposes. The DPDP Act mentions that appropriate technical and organisational measures must be implemented for processing of the personal data and reasonable security safeguards must be taken to prevent any personal data breach.

****