GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 737
TO BE ANSWERED ON: 22.07.2022

DEALING WITH CYBER SECURITY THREATS

737. SHRI HARDWAR DUBEY:

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

(a) the efforts being made by Government to deal with the cyber security threats originating from internet;

(b) whether the data stored on cloud is secure, if not, the details thereof;

(c) the details of efforts made by Government for making data protection strategy and to mitigate and control cyber frauds; and

(d) whether Government has formulated any rules or guidelines for social media platform (Twitter/Facebook) companies, the action taken against such companies by Government on their non-adherence to these rules?

ANSWER

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

(a): The Government has institutionalised a nationwide integrated and coordinated system to deal with the cyber security threats originating from internet which, inter alia, includes:

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

ii. Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents

iii. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.

iv. Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

v. Department of Telecommunications (DoT) has established Telecom Security Operations Centre (TSOC) for effective management of security incidents including prevention, identification and response system for national telecom infrastructure.

(b): Yes, Sir. The security is provided as a fundamental requirement in the Cloud. Security in the Cloud is the shared responsibility between the Cloud Service Providers (CSPs) and the end-users.

The Cloud Service Provider (CSP) ensures security of the underlying infrastructure in the Cloud by complying to the various international Cloud standards. Cloud Service Providers (CSP) are required to go through periodic security audits to ensure that they meet the ever-evolving security guidelines and compliances mandated by the Government of India.

Further, depending on the nature of the applications/data hosted on the Cloud, prescriptive security guidelines/compliances must be put in place by the end-users. Organisations using cloud services are required to make continuous efforts by way of hardening and deploying appropriate security controls, to protect the data stored on cloud infrastructure.

As a part of data protection strategy and to secure cloud infrastructure, NIC uses encryption at data rest as well as at data transient, also NIC undertakes periodic security audits and vulnerability assessment of resources, followed by subsequent hardenings.

(c): Government has taken several measures to enhance the cyber security posture and prevent cyber-attacks:

i. 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.

ii. Government operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing free tools developed in collaboration with industry and research institutions for detection and removal of malicious code and securing computers and mobile devices.

iii. All authorised entities/ banks issuing (Prepaid Payment Instruments) PPIs in the country have been advised by CERT-In through Reserve Bank of India to carry out special audit by empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices

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 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.

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

vii. 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 to ensure safe usage of digital technologies. CERT-In has issued 70 advisories for organisations and users for data security and mitigating fraudulent activities

viii. CERT-In has empanelled 97 security auditing organisations to support and audit implementation of Information Security Best Practices.

ix. Cyber security mock drills are conducted regularly in Government and critical sectors. So far 67 such drills have been conducted by CERT-In where 886 organisations from different States and sectors have participated.

x. CERT-In regularly conducts 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). 134 CCMP workshops have been conducted till June 2022 by CERT-In.

xi. CERT-In regular conducts 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. 19 and 5 training programs have been conducted covering 5169 and 449 participants during the year 2021 and 2022 (till June 2022) respectively.

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

xiii. Security tips have been published by CERT-In to enable users to secure their mobile/smart phones.

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

xv. Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through portals like "www.infosecawareness.in", and "www.cyberswachhtakendra.gov.in".

(d): The Government policies are aimed to ensure Open, Safe&Trusted and Accountable Internet. The Government has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Codes) Rules, 2021 on 25thFebruary, 2021 to make intermediaries including social media platforms accountable to their users and enhance user safety online. The Rules also prescribe the additional due diligence to be followed by significant social media intermediaries (SSMI) having 50 lakh or more registered users in India. In case of non-compliance to the abovesaid rules, the provisions of sub-section (1) of section 79 of the IT Act becomes applicable to such intermediary and the intermediary are liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

****