GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION. NO. *195
TO BE ANSWERED ON: 02.08.2023

CYBER ATTACK INCIDENTS

***195. SHRI KURUVA GORANTLA MADHAV:**

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

(a) the details of cyber attack incidents on Government systems and infrastructure during the last five years;

(b) the estimated loss suffered due to these cyber attacks;

(c) whether the Government has taken any steps to strengthen Government systems and infrastructure against these cyber attacks; and

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

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A Statement is laid on the Table of the House

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. *195 FOR 02.08.2023 REGARDING CYBER ATTACK INCIDENTS

.....

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the expansion of the Internet and more and more Indians coming online, the possibility of cyber-attacks has also increased. Government is fully cognizant and aware of various cyber security threats.

Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported total number of 70798, 85797, 54314, 48285,192439and 112474cyber security incidents related to Government organisations / systems during the year 2018, 2019, 2020, 2021, 2022 and 2023(upto June) respectively.

With innovation in technology and rise in usage of the cyberspace and digital infrastructure for businesses and services, cyber-attacks pose a threat to confidentiality, integrity and availability of data and services, which may have direct or indirect impact on the organisation. Such impact is specific to the impacted entity, and depends on the extent to which its data, assets and services are affected by such attacks.

(c) and (d): The following measures have been taken by Government to set-up requisite infrastructure and schemes to provide for greater security against cyber-attacks:

(i) The National Cyber Security Coordinator under the National Security Council Secretariat coordinates with different agencies at the national level in respect of cybersecurity matters.
(ii) The Government has designated Indian Computer Emergency Response Team (CERT-In) as the national agency for responding to cyber security incidents. 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.
(iii) 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.
(iv) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate situational awareness regarding existing and potential cyber security threats.
(v) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same for citizens and organisations. The centre works in close coordination and collaboration with Internet service providers, academia and industry.
(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
(vii) A Cyber Crisis Management Plan is formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors to help them to counter cyber-attacks and cyber-terrorism.
(viii) Department of Telecommunications (DoT) has established Telecom Security Operations Centre (TSOC) for detection of threats and malicious traffic to facilitate protecting telecom infrastructure of the country.
(ix) Government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.
(x) National Informatics Centre (NIC) provides IT/E-Governance related services to Government Departments. NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies.
(xi) 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. Additionally, NIC issues advisories to Government / NICNET users for taking precautionary measures.

****