GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION 612
TO BE ANSWERED ON: 05.02.2020

CYBER ATTACKS

612. SHRI DHAIRYASHEEL SAMBHAJIRAO MANE:
DR. SUJAY RADHAKRISHNA VIKHE PATIL:
SHRI HEMANT SRIRAM PATIL:
SHRI RANJEET SINGH HINDURAO NAIK NIMBALKAR:
SHRI MANNE SRINIVAS REDDY:
DR. SHRIKANT EKNATH SHINDE:

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

(a) whether the incidents of cyber-attacks in the country have increased in recent years from 49,000 cases in 2015 to 53,000 cases in 2017 and 60,000 in 2018 and if so, the details thereof including the incidents of cyber-attack reported in the current financial year, State/UT-wise and the reasons therefor;
(b) the action taken by the Government in this regard;
(c) whether the reporting of cyber-attacks in the country is very low and taking that into account, the actual figures would be much more and if so, the details thereof and the reasons therefor;
(d) the steps taken by the Government in this regard;
(e) the sectors which are more prone to cyber-attacks; and
(f) the names of the major countries from which cyber attacks on India are majorly emanated and firewalls set by the Ministry to thwart them?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): Cyber space is a complex environment of people, software, hardware and services on the Internet. Due to vulnerabilities in software, lack of awareness amongst people and evolving processes, there are possibilities of increased cyber security incidents. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 49455, 50362, 53117, 208456 and 394499 cyber security incidents are reported during the year 2015, 2016, 2017, 2018 and 2019 respectively. State/UT-wise data is not maintained centrally.

(b): In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect networks by way of hardening and deploying appropriate security controls.

Government has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(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) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(iii) All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.
(iv) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

(v) Government has formulated 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) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

(vii) 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. 23 trainings covering 692 participants conducted in the year 2019.

(viii) Government has launched 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.

(ix) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

(c) and (d): As per mandate of CERT-In under Section 70B of Information Technology Act, 2000 and rules therein, Service providers, intermediaries, data centres and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action. The following type of security incidents shall be mandatorily reported to CERT-In as early as possible to leave scope for action - Targeted scanning/probing of critical networks/systems; Compromise of critical systems/information; Unauthorised access of Information Technology systems/data; Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.; Malicious code attacks such as spreading of virus /worm /Trojan /Botnets /Spyware; Attacks on servers such as Database, Mail and Domain Name System and network devices such as Routers; Identify theft, spoofing and Phishing attacks; Denial of Service and Distributed Denial of Service attacks; Attacks on Critical Infrastructures, supervisory control and data acquisition (SCADA) systems and Wireless networks; Attacks on Applications such as E-Governance, E-Commerce etc.

The incidents are reported to CERT-In by various organisations and individuals. CERT-In has released advertisements in December 2016 in English and Hindi newspapers for creation of awareness regarding reporting of security incidents. Moreover, in various seminars/ training programs organized by MeitY and CERT-In emphasis is given for regular reporting of cyber security incidents to CERT-In.

(e): With the increase in the proliferation of Information Technology and related services there is a rise in cyber security incidents in the country as well as globally. As per the information reported to and tracked by CERT-In cyber security incidents are observed across sectors such as Academia, E-Commerce, Energy, Entertainment, Finance, Government, Healthcare, Information Technology, Manufacturing, Telecom, Transportation etc

(f): There have been attempts from time to time to launch cyber-attacks on Indian cyber space. It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are being launched. According to the logs analyzed and made available to CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, Brazil, China, France, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, USA, Vietnam etc.

****