GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2740
TO BE ANSWERED ON: 12.12.2019

CYBER ATTACKS IN THE COUNTRY

2740. SHRI PRABHAKAR REDDY VEMIREDDY:

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

(a) whether cyber attacks on India are rapidly going up from 49,000 in 2015 to 53,000 in 2017 and 60,000 in 2018;
(b) status of cyber attacks on India till November, 2019;
(c) whether it is also a fact that reporting of cyber attacks in the country is too low and if one takes this into account, the figures would be much more;
(d) details of sectors on which there are more cyber attacks; and
(e) which are the major countries from which India is facing cyber attacks and what firewalls the Ministry has set to thwart them?

ANSWER

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

(a) and (b): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 49455, 50362, 53117, 208456 and 313649 cyber security incidents are reported during the year 2015, 2016, 2017, 2018 and 2019 (till October) respectively.

(c): 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.

(d): 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.

(e): 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 have originated belong to various countries including Algeria, Brazil, China, France, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, USA, Vietnam etc.
In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by concerned entities 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. 19 trainings covering 515 participants conducted in the year 2019 till October.
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.

****