GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 739
TO BE ANSWERED ON: 21.07.2017

CYBER ATTACKS AND PREVENTIVE MEASURES

739 DR. T. SUBBARAMI REDDY:
SHRIMATI AMBIKA SONI:

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

(a) the details of number of cyber attacks that happened in the country in the last three years, year-wise;

(b) the steps taken to ensure cyber security and warnings issued to the corporate sector;

(c) the impact of recent Petya ransomware in the country and proactive measures initiated by Government; and

(d) the details of preventive measures being taken to guard against such attacks in future in view of increasing digitization in the country?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks, etc.

(b): The following actions are taken by the Government to ensure cyber security:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect IT systems and mobile devices. In addition, tailored alerts are being sent to key organisations in public and private sector regarding latest cyber threats and countermeasures.

(ii) 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

(iii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors including Corporate sector. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

(iv) Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.

(v) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 14 training programs covering 431 participants and 13 training programs covering 329 participants were conducted during 2016 and 2017 (till June).

(vi) 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 for banks as well as common users.

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

(viii) CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations to give an exposure on current threat landscape and countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

(ix) Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like http://infosecawareness.in/ and www.cyberswachhtakendra.in

(c) and (d): Propagation of ransomware called Petya has been reported in many countries around the world including India since 27 June 2017. Ransomware is a type of malicious software that infects a computer and restricts users' access to affected files by encrypting them until a ransom is paid to unlock it. As reported to CERT-In, operations of one sea port were partially affected by the Petya ransomware. Remedial measures to contain damage and prevent such incidents have been advised by CERT-In.

The following steps have been taken by the Government to prevent recent ransomware attacks:

i. The Indian Computer Emergency (CERT-In) has issued an advisory regarding detection prevention of WannaCry ransomware on its website on 13 May 2017. Advisory regarding detection and prevention of Petya ransomware was issued by CERT-In on 27 June 2017.

ii. CERT-In has issued a vulnerability note on its website with a Severity Rating of high on March 15, 2017 suggesting information regarding vulnerabilities in Microsoft Windows systems which have been exploited by Wannacry and Petya ransomware alongwith remedial measures.

iii. CERT-In has informed various key organisations across sectors in the country regarding the ransomware threat and advised measures to be taken to prevent the same.

iv. Free tools for detection and removal of ransomware/bots have been provided on the website of Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in).

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

vi. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

****