GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 736
TO BE ANSWERED ON: 21.07.2017

CYBER ATTACKS AND GST NETWORKING

736 SHRI KIRANMAY NANDA:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether Government is aware that during the recent past, a number of cases of major cyber attacks were reported, which have taken entire digital network on task;
(b) if so, whether Government is taking cyber safety measures to combat such attacks;
(c) if so, the details thereof and if not, the reasons therefor; and
(d) whether GST network would also be safe from cyber attackers?

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) and (c) : Government is taking the following cyber safety measures to combat cyber attacks, namely:-

(i) Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
(ii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 15 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 148 organisations from different sectors.
(iii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and mobile phones on regular basis.
(iv) CERT-In is regularly tracking the hacking of websites and alerts the concerned website owners to take actions to secure the websites to prevent recurrence.
(v) All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the hosted websites and applications is conducted on a regular basis after hosting also. CERT-In has empanelled 54 security auditing organizations to support and audit implementation of Information Security Best Practices.
(vi) 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).

(vii) Government has established 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.

(d): The cyber security is part of GST system and a dedicated Security Operations Command Center (SOOC) is operational 24x7x365 as part of GST Network (GSTN). GSTN has been desined with various requisite security features including the following:

(i) Core GST System is not exposed directly to internet and any interaction with GST system is only through Application Programming Interfaces (APIs);

(ii) Multi-layered security architecture;

(iii) Segregation via Virtual Local Area Network (VLANs) / Zoning, Segregation of Duties (SODs), least privilege access principles, IP filtering/blocking rogue IPs, Resiliency at each layer

(iv) Secure Coding practices ensuring security of GST software development throughout Software Development Life Cycle (SDLC);

(v) Data Encryption (at rest and during transit) and Data sharding- Any data transfer from GST System is in encrypted format using AES256/SHA256; and,

(vi) Thorough Security testing i.e. Secure code scanning, static and dynamic Analysis of Open Source components, Full system Vulnerability Assessment and Penetration Testing of IT Infrastructure, Apps using licensed tools and customized scripts.

****