GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3295
TO BE ANSWERED ON: 23.03.2018

RECENT CYBER ATTACKS

3295. SHRI AJAY SANCHETI:

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

(a) the details of recent cyber attacks;
(b) whether this has revealed vulnerability of both businesses and critical national infrastructure; and
(c) if so, the steps proposed to be taken for cyber defence and maintenance of IT infrastructure?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 53081 cyber security incidents were observed during the year 2017. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc.

(b): Over a period, the nature and pattern of incidents have become more sophisticated and complex. In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect servers by way of hardening and deploying appropriate security controls.

(c): Government has taken following measures for preventing cyber attacks and enhancing security of Information Technology infrastructure :

(i) All the new government websites and applications hosted on National Informatics Centre (NIC) are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting. The Indian Computer Emergency Response Team (CERT-In) has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.

(ii) CERT-In is regularly tracking the hacking of websites and alerts the website owners concerned to take actions to secure the websites to prevent recurrence. CERT-In also issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

(iii) Government has formulated Cyber 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.

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

(v) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated.

(vi) 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. 22 training programs covering 610 participants were conducted during the year 2017.

(vii) 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.

(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.

*****