GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1847
TO BE ANSWERED ON: 07.03.2018

MISUSE OF SERVERS BY CYBER CRIMINALS

1847. SHRIMATI RANJANBEN BHATT:

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

(a) whether a number of servers are being misused by cyber criminals in the country;

(b) if so, whether the Government is considering to take any concrete and effective steps to stop this malpractice; and

(c) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a): Organisations use servers to host websites and applications for dissemination of information and providing services to users. The servers not configured properly and having vulnerable software are prone to hacking and could be misused by cyber criminals. 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.

(b) and (c): Government has taken various steps for preventing cyber attacks and enhancing the cyber security of information technology infrastructure in the country, these are:

i. All the new government websites and applications are to be 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. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers/servers on regular basis.

iv. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 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. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

v. 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.

vi. Government has initiated setting up of 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.

vii. 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.

viii. National Information Centre (NIC), which provides IT / E-Governance related services to Government departments protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the–clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.

****