GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2048
TO BE ANSWERED ON: 07.03.2018

CYBER ATTACKS ON PORTALS

2048. SHRI ANURAG SINGH THAKUR:

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

(a) the number of cyber attacks on Indian portals in 2017-18 (please classify them as governmental/others, websites/ apps, malware /ransomware/ hacking, payment gateway attacks etc.);

(b) the number of attacks forecasted and alerted by Computer Emergency Response Team-India in 2017-18; and

(c) the measures undertaken by the Government to prevent and mitigate all kinds of cyber threats, including cyber attacks?

ANSWER

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

(a): As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In) a total of 22,207 Indian websites including 114 Government websites were hacked during April 2017 to January 2018. A total number of 493 affected websites were used for malware propagation.

Further, As per the information reported to and tracked by National Informatics Centre (NIC), a total number of 74 and 6 Government websites hosted on NICNET were hacked during the year 2017 and 2018 (till February) respectively.

(b): A total of 301 security alerts regarding potential vulnerabilities and threats to multiple systems and applications were issued by CERT-In during April 2017 to January 2018. In addition, various tailored alerts were sent to key organisations to enable them to detect and prevent cyber attacks.

(c) Government has taken various measures for preventing cyber security incidents and enhancing the cyber security of information technology infrastructure in the country. These are:

i. Information Technology Act, 2000 has adequate deterrent provisions for cyber threats and cyber attacks.
ii. 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.

iii. 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.

iv. 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.

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

vi. 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.

vii. 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.

viii. 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.

ix. 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.

x. 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.

xi. 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. Also, relevant advisories are circulated among the NICNET users for taking precautionary measures from time-to-time. 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 hardenings. These are complemented by round-the-clock monitoring of security events.

*****