GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2005
TO BE ANSWERED ON: 23.12.2022

HACKING OF INDIAN SERVERS BY HACKERS FROM VARIOUS COUNTRIES

2005. SHRI K.R.N. RAJESHKUMAR:

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

(a) whether it is a fact that various Indian servers have been hacked by hackers from various countries;

(b) if so, the details of the incidents and the revenue impact thereof; and

(c) the steps taken by the Ministry to prevent such incidents?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With a borderless cyberspace, coupled with the anonymity, rapid growth of Internet, rise in cyber security incidents is a global phenomenon. Government is fully cognizant and aware of various cyber security threats.

There have been attempts from time to time to launch cyber-attacks on the Indian cyberspace from outside the country. It has been observed that such attacks compromised computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are launched.

With innovation in technology and rise in usage in the cyberspace and digital infrastructure for businesses and services, cyber-attacks pose a threat to confidentiality, integrity and availability of information and services, which may have indirect or direct impact on the revenues of businesses and service providers. Such revenue impact is specific to the impacted entity, and depends on the extent to which its assets and services are affected by such attacks.

(c): The following measures have been taken to enhance the cyber security posture and curb such incidents:

(i) The Indian Computer Emergency Response Team (CERT-In)coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies. CERT-In notifies the affected organisations along with remedial actions to be taken.
(ii) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
(iii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.
(iv) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
(v) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

(vi) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.

(vii) Cyber Crisis Management Plan formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors help to counter cyber-attacks and cyber terrorism.

(viii) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. 41 training programmes have been conducted, covering 11,377 participants, during the years 2021 and 2022 (up to November).

(ix) All government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

(x) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. Seventy four such drills have been conducted by CERT-In, covering 990 organisations from different States and sectors.

(xi) CERT-In and the Reserve Bank of India jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

(xii) CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

(xiii) CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as law enforcement agencies.

(xiv) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(xv) The analytics centre at National Critical Information Infrastructure Protection Centre provides near-real-time threat intelligence and situation awareness, based on which regular alerts and advisories are sent to critical information infrastructure / protected system entities to mitigate cyber security threats.

****