GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1223
TO BE ANSWERED ON: 16.12.2022

HACKING OF AIIMS SERVER

1223. DR. JOHN BRITTAS:

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

(a) whether it is a fact that servers of AIIMS have been hacked by ransomware;
(b) if so, the details thereof;
(c) the quantum of data that has been compromised; and
(d) the steps that have been taken to prevent such incidents?

ANSWER

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

(a) and (b): The All India Institute of Medical Sciences (AIIMS) information and computer systems were managed by AIIMS themselves and upon being informed about cyber security incident by AIIMS, the Indian Computer Emergency Response Team (CERT-In) has done evaluation of the incident. As per preliminary analysis, servers were compromised in the information technology network of AIIMS by unknown threat actors due to improper network segmentation, which caused operational disruption due to non-functionality of critical applications. CERT-In and other stakeholder entities have advised necessary remedial measures.

(c): Based on current analysis by concerned stakeholders, 5 servers of AIIMS were affected and approximately 1.3 Tera Bytes of data was encrypted.

(d):The following measures have been taken to enhance the cybersecurity posture and curb such incidents:

(i) CERT-In is mandated to track and monitor cyber security incidents in India. A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cybersecurity threats. The Ministry has been requested to disseminate the advisory among all authorised medical care entities/ service providers in the country. It has also been suggested that they may carryout special audit through CERT-In-empanelled auditors on priority basis, comply with the findings of such audit and ensure implementation of security best practices.

(ii) On observing a ransomware incident, CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.

(iii) A Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, has been formulated by CERT-In, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

(iv) Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for securing the information technology infrastructure and mitigating cyber-attacks. A total of 41 training

programmes were conducted, covering 11,377 participants, during the years 2021 and 2022 (up to November).

(v) CERT-In has been issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis. It has also published "India Ransomware Report H1 – 2022" in August 2022, covering latest tactics and techniques of ransomware attackers and ransomware-specific incident response and mitigation measures.

(vi) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is operated by CERT-In to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(vii) 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.

(viii) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from different States and sectors participated.

(ix) The National Cyber Coordination Centre has been set up to generate situational awareness regarding existing and potential cyber security threats.

****