GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2310
TO BE ANSWERED ON: 21.12.2022

CYBER ATTACK IN AIIMS

2310. SHRI ARUN SAO:
SHRI MOHAN MANDAVI:
SHRI SUDHAKAR TUKARAM SHRANGARE:
SHRI VIJAY BAGHEL:
SHRI DEVJI M. PATEL:
SHRI SUNIL KUMAR SINGH:
SHRI KUMBAKUDI SUDHAKARAN:
SHRI SUNIL KUMAR SONI:
SHRI RAM MOHAN NAIDU KINJARAPU:
SHRI RAKESH SINGH:
SHRI V.K. SREEKANDAN:

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

(a) whether it is a fact that the All India Institute of Medical Science (AIIMS) suffered a cyber attack recently in which the medical data of lakhs of patients including high ranking Government functionaries and diplomats have been stolen by hackers;

(b) if so, the details thereof including the total number of patients whose data have been stolen;

(c) the details of the cases of similar Ransomware targeting commercial and critical infrastructure that have been reported in the recent past including the hacking of Ministry of Jal Shakti Twitter account;

(d) whether the Government has identified the culprits behind the cyber attack of AIIMS, if so, the details thereof and if not, the reasons therefor;

(e) whether the Government has made concrete efforts taken measures to prevent such cyber attack and check increasing cyber crime in future; and
(f) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) and (b):The Information and computer systems of AIIMS are managed by AIIMS. Upon receipt of information about the occurrence of a cyber security incident from AIIMS, the Indian Computer Emergency Response Team (CERT-In) has carried out an evaluation of the incident. As per preliminary analysis, servers in the information technology network of AIIMS were compromised 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. Based on current analysis by concerned stakeholders, five servers of AIIMS were affected.
(c): The Twitter account of the Ministry of Jal Shakti was compromised recently and fraudulent crypto related tweets were posted. CERT-In advised the Ministry on necessary remedial measures to secure its social media accounts.

Ransomware incidents have grown over time with attacks across multiple sectors, including commercial and critical infrastructure. Threat actors have modernised their attack methodologies, evolved sophisticated tactics and adopted a wide range of attack campaigns. Ransomware actors exploit known vulnerabilities, compromised credentials of remote access services and phishing campaigns for gaining access into the infrastructure of organisations.

(d): As per AIIMS, an FIR was registered under section 385 of the Indian Penal Code and section 66 and 66F of Information Technology Act,2000 with the Special Cell of Delhi Police, and the affected physical servers were seized by the Special Cell for investigation.

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

(i) 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 cyber security 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 carry out 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) Cybersecurity mock drills are conducted to enable assessment of cybersecurity 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.

****