GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1743
TO BE ANSWERED ON: 27.07.2022

CYBER ATTACKS

1743. SHRIMATI VANGA GEETHA VISWANATH:
DR. ARVIND KUMAR SHARMA:
SHRI G.M. SIDDESHWAR:

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

(a) whether India is among one of the most cyber attack targeted countries in the world especially by China and if so, the details thereof including the efforts being made to address the situation;

(b) whether any security policies have been introduced by the Government during the last three years to strengthen the cyber security of the country, if so, the details thereof including the progress made there under and if not, the reasons therefor; and

(c) whether any measures have been taken by the Government during the last three years to restrict data theft of an individual and if so, the details thereof?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. With over 80 crore Indians connected to the internet, India is one of the largest connected nations in the world.

With the borderless cyberspace coupled with the anonymity, along with rapid growth of Internet, rise in cyber security incidents is a global phenomenon. Further, there has been media articles, citing a report published by IBM X-Force (A threat intelligence sharing platform) in year 2022, stating that India was one of the most Cyber attacked country in Asia. The findings of such reports by cyber security vendors are generally based on data generated by their products and details of such data is not available and hence cannot be verified.

As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), a total number of 11,58, 208, 14,02,809 and 6,74,021 cyber security incidents have been observed during the year 2020, 2021 and 2022 (upto June) respectively.

According to the logs analyzed and made available to Indian Computer Emergency Response Team (CERT-In), the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including China.

(b): Government has formulated a draft National Cyber Security Strategy (NCSS) which holistically looks at addressing the issues of security of national cyberspace. The vision of the Cyber Security Strategy is to “Ensure a safe, secure, trusted, resilient and vibrant cyber space for India’s prosperity”.

Ministry of Home Affairs (MHA) has issued National Information Security Policy and Guidelines (NISPG) to the Central Ministries/Departments as well as the State Governments/Union Territories in order to prevent information security breaches/Cyber intrusions in ICT infrastructure.

The cyber security policy for National Informatics Centre Network (NICNET) is in place.

(c): Government has taken following measures to enhance cyber security and mitigate data breaches:

(i) Indian Computer Emergency Team (CERT-In) issues advisories to organizations regarding prevention of data breaches, data leaks and best practices to be followed by users for mitigating risks due to data breaches and securing online credentials. CERT-In has issued 70 advisories for data security and mitigating fraudulent activities. Further, CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
(ii) CERT-In operates an automated cyber threat exchange platform to proactively collect, analyse and share tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
(iii) Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.
(iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(v) All the government websites and applications are audited with respect to cyber security prior to their hosting. The audit of the websites and applications is conducted on a regular basis after hosting also.
(vi) CERT-In has empanelled 97 security auditing organisations to support and audit implementation of Information Security Best Practices.
(vii) CERT-In has formulated a Cyber Crisis Management Plan to counter cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
(viii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 67 such drills have so far been conducted by CERT-In where 886 organizationsfrom different States and sectors participated.
(ix) 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. 19 and 5 training programs were conducted covering 5169 and 449 participants during the year 2021 and 2022 (upto June) respectively.
(x) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same alongwith cyber security tips and best practices for citizens and organisations.
(xi) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

(xii) 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.
(xiii) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Cyber Security Awareness Month in October 2021 and Safe Internet day on 8 February 2022 by posting security tips using posters and videos on social media platforms and websites. CERT-In in association

with CDAC conducted online awareness campaign for citizens covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices etc. through videos and quizzes on MyGov platform.

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

(xv) Ministry of Electronics & Information Technology (MEITY) conducts programs 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 like "www.infosecawareness.in", and www.csk.gov.in.

(xvi) National Informatics Centre (NIC) adopts layered security approach in the form of practices, procedures an technologies that are put in place at both Network and Application level, in order to protect sensitive information. This is further strengthened through periodic compliance, audit and vulnerability assessment.

****