Cyberwarfare signs: Govt alerts industry

Large groups, MSMEs asked to step up defences

AASHISH ARYAN
New Delhi, 16 May

The government is on high alert amid the threat of a cyberwarfare against Indian digital establishments and resources. Even as the India-Pakistan tension has de-escalated, the government is watching out for international ransomware groups and state-backed threat actors, who could step up their attempts to attack in the coming days and weeks, sources told *Business Standard*.

To take the threat head on, the Ministry of Electronics and Information Technology (Meity) is reaching out to software firms, cybersecurity experts, chief information officers at large industrial groups, as well as micro, small, and medium enterprises (MSMEs), sources said.

A new set of guidelines to ensure cybersecurity compliance has also been sent to industry stakeholders. The guidelines come along with instructions to report any incidents, minor or major, to the government, as well as a regular compliance audit structure, said a senior government official who did not wish to be named.

In case of any recorded cyberattacks, companies have been asked to ensure rapid detection and restoration of "public-facing assets in case of website-defacement attacks", and preserve all logs of the incident to ensure a third-party audit, if needed, the official pointed out.

The government alert has been prompted by a rise in cyberattack cases during and after Operation Sindoor. Following the terrorist attack on tourists in Pahalgam and the subsequent Operation Sindoor, more than one million cybersecurity incidents were flagged within 10 days. These included state-sponsored actors like APT36 and numerous hacktivist groups, industry experts said.

Some of these attacks were recorded using advanced and sophisticated spear-phishing campaigns using malware like CrimsonRAT and MeshAgent, said Tarun Wig, the cofounder of Innefu Labs, a cybersecurity firm.

Looking ahead, the Indian Computer Emergency Response Team (Cert-In) has sent an updated advisory to large data fiduciaries as well as MSMEs on cyber defence mechanism.

Turn to Page 6

On guard

Cert-In's advisory to:

LARGE DATA FIDUCIARIES

- Tighten authentication and access controls
- Use automated tools to update systems with latest software and security patches
- Continuously scan infrastructure for vulnerable ports; isolate or remove outdated systems
- Monitor third-party/vendor software for unauthorised updates or configurations

MSMEs

- Use strong alphanumeric passwords, anti-virus/malware tools, and conduct regular cybersecurity training

BOTH

- Maintain regular offline backups
- Consider zero-trust architecture with multi-layer identity verification and authorisation

Implement a zero-trust architecture: Cert-In to data fiduciaries, MSMEs

Large data fiduciaries should strengthen authentication and access control to their digital systems, use automated tools to regularly update the systems with the latest software and security protocols, run continuous infrastructure scans for all possible vulnerable ports, and isolate or remove old digital infrastructure, Cert-In has conveyed to them.

"We have also asked all large companies and enterprises to monitor all incoming and outgoing data, use encryption as much as possible during data transmission, and implement advanced DLP (data loss prevention) solutions," an official emphasised.

Companies that depend on third-party and vendor-based software solutions have been asked to monitor any unauthorised software and system configuration updates.

MSMEs have been advised to follow cost-effective measures, such as using strong, complex passwords with alphanumeric characters, using antivirus and antimalware solutions, and conducting regular cybersecurity training for employees, it is learnt.

Both big data fiduciaries and MSMEs have also been asked to maintain regular offline backups for their critical data components. Implementing a zero-trust architecture by verifying every access request through multilayer identity verification and authorisation processes is another step that has been recommended.

While MSMEs may not be able to ramp up their defence mechanisms so quickly, the government is making efforts to guide them, said one of the officials quoted above.

Critical national infrastructure, such as the energy and telecom installations, banking, financial services, and insurance, must be particularly vigilant now, said Kartik Shinde, a partner of the cybersecurity consulting practice at EY India.

"They should anticipate sustained and potentially more sophisticated attacks, potential exploitation of any breached data for secondary attacks like targeted phishing, and continued disinformation campaigns. Implementing robust technical controls, enhancing employee cyber hygiene, and sharing threat intelligence are crucial defences," Shinde said.