Source : www.livemint.com Date : 2021-03-09

INDIA PLANS NEW NATIONAL STRATEGY ON CYBERSECURITY AMID CHINA HACKING CONCERNS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

The plan will coordinate responses across ministries including home affairs, IT, defense and the National Critical Information Infrastructure Protection Centre in case of an attack and set audit procedures, former Lt General Rajesh Pant, India's National Cyber Security Coordinator said

India is mulling a new national strategy to strengthen the country's cybersecurity amid allegations that Chinese intrusions may have affected operations at a key stock exchange and supply of electricity in the country's commercial capital.

The plan will coordinate responses across ministries including Home Affairs, Information Technology, Defense and the National Critical Information Infrastructure Protection Centre in case of an attack and set audit procedures, former Lieutenant General Rajesh Pant, India's National Cyber Security Coordinator said in an interview. It will be approved by the cabinet committee on security headed by Prime Minister Narendra Modi.

Authorities are investigating a series of recent suspected cyber intrusions which could have led to a power outage in Mumbai, crippled systems at banks and caused a glitch at the country's premier National Stock Exchange, he said. The report is expected in about a fortnight.

"We also want to know what happened," said Pant, who served in the Indian army and now coordinates India's cyber intelligence and reports to the Prime Minister's Office. He said the breaches were likely malware and couldn't be classified as attacks without a proper investigation.

At least one connection opened by Chinese state-sponsored hackers into the network system of an Indian port was still active, as authorities blocked attempts to penetrate the South Asian nation's electrical sector, the U.S.-based research firm Recorded Future said last week. The attempts by the Red Echo group have been occurring since at least the middle of last year, around the time a bloody skirmish between Indian and Chinese soldiers started in the remote Himalayan region, the firm said.

The new strategy will lay down protocols for prevention and audit to secure the government's digitally connected water, health and education systems that are all being treated as critical infrastructure, he said. Infrastructure like nuclear, power and aviation will be considered supercritical.

"In my view, if internet-connected computers are infected by malware, I won't say it's an attack but an infection unless it jumps from IT systems to other operation systems," Pant said. "It's like a crank caller. Can you stop someone from dialing your number?"

Your session has expired, please login again.

You are now subscribed to our newsletters. In case you can’t find any email from our side, please check the spam folder.

END