Business Standard

Vulnerabilities in India's digital infra spur rise in cyberattacks: Experts

SaaS and conglomerate companies experienced ten times more attacks than the preceding quarter, according to the study

A large digital footprint and vulnerabilities in India's technological infrastructure due to the rapid pace of deployment are the reasons why India is witnessing an increasing number of cyberattacks in recent times, say experts.

"The rapid pace of digital transformation in India has sometimes resulted in the deployment of complex technological infrastructures with inherent vulnerabilities. Weaknesses in these systems can make them attractive targets for cyberattacks," said Kumar Ritesh, founder and CEO, Cyfirma.

India witnessed a 70 per cent rise in cyberattacks in Q3 this year, with more than 1.6 billion blocked attacks across the globe originating from the country, according to a recent study by Indusface.

The State of Application Security Report by Indusface said that around 90 per cent of India's banking and insurance sector faced bot attacks in the third quarter of this year.

"With the government's push towards a cashless economy, there has been a surge in digital payment transactions. This has attracted the attention of cybercriminals who seek to exploit vulnerabilities in payment systems and steal sensitive financial information," added Ritesh.

SaaS and conglomerate companies experienced ten times more attacks than the preceding quarter, according to the study.

In Q3, eight out of ten sites found themselves targeted by bot attacks, and the number of overall bot attacks was 56 per cent higher compared to the previous quarter. Further, almost every website falling under the healthcare domain faced bot attacks during this quarter.

Cybersecurity experts believe that the increased use of big data and AI has led to 'hoarding' of data with the hope of monetising it in the future, leading to an increase in the number of cyberattacks in India.

"With the advent of big data and AI, organisations have been hoarding humongous amounts of data with the hope to monetise it in the future, with diminishing ownership and accountability with its internal business owners. This has led to many high-profile incidents across the world," said Vishal Salvi, CEO, Quick Heal Technologies.

"The provisions of the DPDP Act will establish accountability for misuse of personal data and also help organisations reduce their attack surface by enforcement of data retention and purging policies," he added.

The report found India, the United States, the United Kingdom, Russia, and Singapore as the major source countries of cyberattacks across the globe.

"Around 46,000 vulnerabilities were identified during Q3, with a concerning 32 per cent remaining unaddressed for over 180 days, underscoring the urgency for immediate action," says the report.

To mitigate the increasing number of cyberattacks in India, cybersecurity experts call for the use of artificial intelligence (AI), large language models (LLM), and Machine Learning (ML) to develop intelligent systems that are capable of identifying and responding to cyber threats autonomously.

These technologies can adapt to new patterns and trends in data, providing a dynamic defence against cyberattacks, say experts.