Healthcare industry faces rising cybersecurity threats: Seqrite report

Malware detections in the healthcare sector were dominated by Trojans, which accounted for 43.38 per cent of all threats

(Pic: hcghospitals.in)

Aneeka Chatterjee Bengaluru

Seqrite, the security arm of Quick Heal, has revealed in a recent report that India's healthcare sector has emerged as the most targeted industry for cyber threats. A report by Seqrite Labs, in partnership with the Data Security Council of India (DSCI), highlighted a pressing concern where healthcare accounted for 21.82 per cent of all detected cyber threats in 2024, surpassing other high-risk sectors such as hospitality (19.57 per cent) and banking, financial services, and insurance (17.38 per cent).

The report, titled India Cyber Threat Report 2025, highlights that the healthcare industry recorded the highest average of 37.29 detections per endpoint among all analysed sectors. This surge is attributed to factors including the sensitive nature of medical data, reliance on outdated systems, and the accelerated digitisation of healthcare services, such as electronic health records and telemedicine platforms.

Malware detections in the healthcare sector were dominated by Trojans, which accounted for 43.38 per cent of all threats. Infectors followed at 34.23 per cent, while worms constituted 8.43 per cent.

Malicious programs frequently exploit vulnerabilities in legacy systems or employ phishing tactics to infiltrate networks. The report further highlights that while ransomware accounts for only 0.30 per cent of detections, it poses a significant threat due to its capacity to disrupt critical healthcare operations.

Emerging threats to the healthcare sector include advanced persistent threats (APTs), vulnerabilities in the Internet of Medical Things (IoMT), supply chain attacks, and AI-driven assaults. These threats exploit the growing digitisation and interconnectivity of healthcare systems, creating substantial risks to patient data and critical healthcare services.

Seqrite recommends “conducting regular security audits, employee training on cybersecurity best practices, implementation of advanced threat detection systems, and collaboration with cybersecurity firms.” The findings underscore the critical need for the healthcare industry to prioritise cybersecurity investments and strengthen defences against the growing tide of cyberattacks.

Geographically, Telangana recorded the highest detection rate in India, with 55.90 detections per endpoint, followed by Tamil Nadu and Delhi. The report also highlights the vulnerability of major urban centres, with Surat leading at 69.34 detections per endpoint, followed by Bengaluru and Jaipur. The prominence of these regions reflects their advanced digital infrastructure and high concentration of technology-driven industries, which inadvertently increases their exposure to cyber risks.

As India dives further into digital transformation, protecting critical infrastructure, including healthcare systems, becomes paramount for national security and public health, the report noted.

According to media reports, some of the most critical cyberattacks in the history of Indian healthcare include the 2020 breach at the All India Institute of Medical Sciences (AIIMS) in Delhi, which caused a prolonged system outage. Sensitive patient data, including medical records, was compromised, exposing gaps in the institution's cybersecurity infrastructure and preparedness.

Additionally, during the pandemic, data breaches involving COVID-19 test results and patient information were reported. The healthcare system also witnessed the Apollo Hospitals data breach in 2021, caused by a vulnerability in a third-party application. In this case, personal details of over 12 million patients were exposed, including names, addresses, phone numbers, and medical records.