Source : www.thehindu.com Date : 2023-05-26

EDUCATION SECTOR WORST HIT AS RANSOMWARE ATTACKS RISE IN INDIA: REPORT

Relevant for: Science & Technology | Topic: Science and Technology- developments and their applications and effects in everyday life

May 25, 2023 01:01 pm | Updated 02:33 pm IST

The rate ransomware attacks increased in India, with 73% of organisations surveyed reporting they were a victim of a ransomware attack, up from 57% the previous year.. | Photo Credit: Getty Images

The rate ransomware attacks increased in India, with 73% of organisations surveyed reporting they were a victim of a ransomware attack, up from 57% the previous year.

In 77% of attacks, organisations reported adversaries succeeded in encrypting data with 44% paying the ransom to get their data back, a considerable drop from last years' rate of 78%.

The education sector was found to be the worst hit globally, with 79% of higher education organizations surveyed and 80% of lower education organizations surveyed reporting that they were victims of ransomware attacks.

Overall, 46% of organisations surveyed that had their data encrypted paid the ransom. Organisations with larger revenues were found to be more likely to pay the ransom.

(For top technology news of the day, subscribe to our tech newsletter Today's Cache)

The survey conducted by Sophos, a cybersecurity company, for its State of Ransomware 2023 report also showed when organisations paid a ransom to get their data decrypted, they ended up doubling their recovery cost - compared to organisations that used backups to get their data back.

Recovery times were also found to be longer for organisations that paid the ransom. 45% of organisations that used backups were able to recover their data within a week, compared to 39% of those that paid the ransom.

Incident costs rise significantly when ransoms are paid, with most victims being unable to recover all their files by simply buying the encryption key. Organisations must rebuild and recover from backups as well, Chester Wisniewski, field CTO, Sophos said.

Analysis of the cause of successful ransomware attacks revealed that exploited vulnerabilities

were the culprit in 35% of the cases while compromised credentials were used in 33% of the cases.

“With almost three quarters of Indian organizations reporting that they have been victimized by ransomware criminals, a lot of work needs to be done. The key to lowering this number is to work to aggressively lower both time to detect and time to respond. Human-led threat hunting is very effective at stopping these criminals in their tracks, but alerts must be investigated, and criminals evicted from systems in hours and days, not weeks and months”, Wisniewski said.

The report is based on vendor-agnostic survey of 3,000 cybersecurity/IT leaders conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA and Asia Pacific and Japan.

END