Qilin Ransomware Attack on Synnovis Led to 6000+ Appointments Cancelled

The Qilin ransomware attack on the pathology services provider Synnovis has significantly impacted the NHS Trusts in central London. Over the past five weeks, the repercussions of this cyber incident have resulted in the cancellation of more than 6,000 appointments and procedures. This article delves into the attack's impact on healthcare services, the ongoing recovery efforts, and the broader implications for the NHS.

Impact on Appointments and Procedures

The two NHS Trusts most heavily impacted by the Qilin ransomware attack, Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust, have faced severe disruptions. According to NHS England London, the week ending 7 July 2024 saw 1,286 acute outpatient appointments and 100 elective procedures postponed. Over the past five weeks, these numbers have escalated to a total of 6,199 acute outpatient appointments and 1,491 elective procedures being cancelled. This disruption has been particularly distressing for patients whose medical needs are urgent, including cancer treatments and organ transplants.

Efforts Towards Recovery

Despite the severe impact, there are signs of improvement. Chris Streather, NHS London medical director, noted a reduction in the number of postponed appointments and procedures. For instance, 136 elective procedures were postponed last week, a significant decrease from the 814 cancellations in the first week of the cyberattack. However, the recovery is gradual and ongoing. Pathology services in south-east London are currently operating at 54% capacity, with blood tests being the most affected. Efforts are being made to prioritise critical referrals and restore services, with a near-normal service resuming for histology and cervical smears.

Broader Implications and Future Measures

The Qilin ransomware attack has exposed vulnerabilities within the NHS's cyber infrastructure. Synnovis, a joint venture involved in this attack, has suffered a major data breach, compromising sensitive information. The organisation works closely with NHS England's Cyber Operations Team and the National Cyber Security Centre to investigate and restore systems. This incident underscores the need for robust cybersecurity measures within healthcare systems. Synnovis has begun implementing new middleware and enlisting global support to improve testing capacity and infrastructure resilience.

The Qilin ransomware attack has profoundly impacted the NHS Trusts in central London, disrupting thousands of medical appointments and procedures. While recovery efforts are showing progress, the path to complete restoration is long and arduous. This incident highlights the critical importance of cybersecurity in healthcare and the need for continuous improvements to protect sensitive patient data and ensure the resilience of medical services. As the investigation and recovery continue, the focus remains on minimising patient disruption and enhancing the security of NHS systems against future threats.

Source: ComputerWeekly

Image Credit: iStock

Published on : Thu, 18 Jul 2024