HealthManagement
Promoting Management and Leadership

Ransomware Puts 100 Romanian Hospitals Offline

In a significant cybersecurity incident, Romanian officials have reported a ransomware attack on the Hippocrate platform, essential for the operation of IT infrastructure across multiple healthcare facilities, leading to disruption in over 100 hospitals. The cyberattack, occurring on the evening of February 11, compromised production servers, encrypting vital files and databases, thus rendering them inaccessible to the affected medical institutions. Initial reports indicated that 21 hospitals were directly affected, a figure that increased to 25 by the following morning. Additionally, 79 other institutions preemptively disconnected their systems as a precautionary measure while further investigations are carried out.

The National Cybersecurity Directorate (DNSC) of Romania, in an update on February 13, stated that there has been no evidence of data theft thus far. Nevertheless, the incident's reach has expanded, affecting four more hospitals. The ransom demand is set at 3.5 Bitcoin (BTC) (equivalent to approximately to Euro 150,000), though the identity of the attackers remains unknown.

The DNSC's advice is clear: "Both the Directorate and other cyber security authorities involved in the analysis of this incident recommend not to contact the attackers and not pay the demanded ransom!" Furthermore, the DNSC advises all hospitals using the compromised Hippocrate technology to isolate the impacted systems from wider networks and the internet without shutting them down, to preserve potential evidence. Restoration efforts should employ data backups after thorough system cleanses, ensuring all software is up-to-date.

The rise in ransomware attacks targeting healthcare systems has been noted by cybersecurity experts. Javvad Malik of KnowBe4 emphasizes the growing threat: "Attacks against healthcare systems have been growing. Unfortunately, it's one of the continuing stark reminders of the necessity for robust cybersecurity measures, regular system updates, and backups. Responding to such attacks requires a coordinated effort, not just in the immediate technical response, but in long-term strategies such as building a strong security culture to bolster resilience against future attacks. Cybersecurity is not just an IT issue; it's a fundamental component of patient care."

Similarly, Tim Mackey from the Synopsys Software Integrity Group highlighted the high stakes for healthcare providers, pointing out the critical nature of protecting patient health information (PHI) from cybercriminals:

"Healthcare providers represent a high-value target for cyber criminals. If the attacker is able to gain write access to any healthcare database, then they have the ability to modify patient information in ways that could impact the life of a patient while also being difficult to undo."

This incident underscores the critical need for robust cybersecurity defenses, ongoing system maintenance, and the importance of a cohesive security culture within the healthcare industry to mitigate future threats.

Source: Forbes

Image Credit: iStock

Published on : Wed, 14 Feb 2024