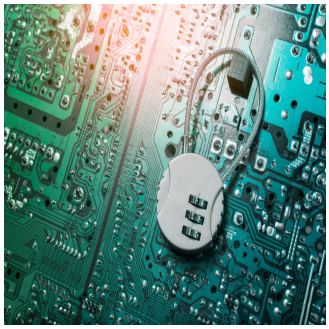
HealthManagement
Promoting Management and Leadership

LockBit Ransomware Targets Croatia's Largest Hospital



In a significant cybercrime incident, the LockBit ransomware gang has claimed responsibility for a cyberattack on Croatia's largest hospital, the University Hospital Centre (KBC) in Zagreb. This breach disrupted the hospital's IT systems, impacting patient care and internal operations. The attack, part of a broader surge in cyberattacks in Croatia, underscores the growing threat of cybercrime in critical infrastructure.

The Impact of the Attack on KBC Zagreb

The cyberattack on KBC Zagreb last week forced the hospital to shut down its IT systems for a day. This shutdown had severe repercussions on hospital operations, particularly emergency services. According to local reports, the incident compelled the hospital to divert patients to other institutions within Zagreb. The assistant director for healthcare quality and supervision at KBC Zagreb, Milivoj Novak, lamented that the attack set them back "50 years — to paper and pencil." The most critical impact was felt in the radiological system, which relies heavily on digital infrastructure.

Response and Investigation

More than 100 specialists worked tirelessly to restore the hospital's systems. However, the damage had already been done, slowing down essential services and jeopardising patient care. LockBit claimed to have accessed sensitive information, including patient and employee data, medical records, and contracts with external entities. Despite these claims, Interior Minister Davor Bozinovic refrained from disclosing details from the ongoing investigation. Health Minister Vili Beros emphasised that the government would not negotiate with the hackers, indicating that monetary gain was likely the motive behind the attack. The full extent of the data breach remains under forensic investigation.

Broader Context of Cyberattacks in Croatia

This incident is not isolated. Croatia has been experiencing a surge in cyberattacks, particularly since the onset of the Russia-Ukraine conflict in 2022. Deputy Prime Minister Tomo Medved highlighted that Croatian institutions face cyberattacks almost daily. Prior to the KBC Zagreb incident, several state institutions, including the Ministry of Interior and the tax service, suffered distributed denial-of-service (DDoS) attacks, claimed by the Russia-linked hacker group NoName057(16). These attacks have raised significant concerns about Croatian institutions' cybersecurity preparedness.

The cyberattack on KBC Zagreb by the LockBit ransomware gang illustrates the profound vulnerabilities in critical healthcare infrastructure. As Croatia grapples with an escalating number of cyberattacks, there is an urgent need for enhanced cybersecurity measures and international cooperation to combat these threats. The ongoing investigations will determine the full impact of the breach, but this incident serves as a stark reminder of the critical importance of robust cybersecurity defences in protecting sensitive information and maintaining essential services.

Source: The Record

Image Credit: iStock

Published on : Wed, 3 Jul 2024