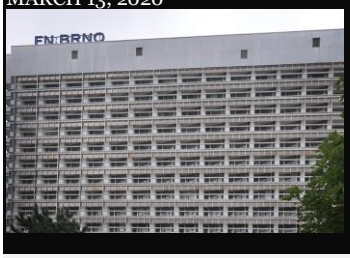
Czech Republic's Second-Biggest Hospital is Hit by Cyberattack

BY PRAGUE MORNING
MARCH 13, 2020



As countries around Europe enact drastic measures to try to contain the spread of the Covid-19 coronavirus, the main hospital in Brno has been forced to cancel all planned operations and farm out acute patients to other hospitals after falling victim to a major cyber attack.

At the time of writing, according to local media reporting, the exact nature of the attack on University Hospital Brno was unknown, but it is understood that hospital staff have had to turn off IT systems, suggesting that its infrastructure may have been encrypted by ransomware.The incident was confirmed by the Czech National Office for Cyber and Information Security (NÚKIB). In a statement on its website, a spokesperson said NÚKIB was notified about the incident on the morning of 13 March.

At present, the spokesperson said, NÚKIB cybersecurity specialists are working alongside police and hospital management to resolve the incident.

Hospital director Jaroslav Štěrba told Czech media that some key clinical systems were working, but the hospital had lost the ability to transfer information from these systems to its database system. He said he hoped it would be possible to quickly identify the nature of the incident and restore systems quickly.

The incident highlights the opportunistic nature of cyber criminal groups and their willingness to demonstrate utter callousness in targeting hospitals on the front line of the fight against the coronavirus.

"Healthcare workers or administrative staff are low-hanging fruit for today's opportunistic hackers," said Jake Olcott, vice-president of government affairs at risk management firm BitSight. "As they seek answers to important questions in a time of crisis, these employees may be susceptible to a hoax email that appears to come from a trusted government body. This is hugely problematic for healthcare companies that are already struggling to reduce cyber security risk.

The hospital is managed by the country's health ministry, according to its website. The facility has been conducting regular tests for the novel coronavirus.

Petr Špiřík, a Prague-based cyber-incident responder with PricewaterhouseCoopers, said the incident was part of a broader pattern of cyberattacks on a vulnerable sector.

"The root cause for this rising level of successful attacks against our hospital sector [and public sector in general] is the overall underfunding in the IT security infrastructure," Špiřík said. That means outdated systems that are vulnerable to attackers.