Nov 7, 2020 eandt.theiet.org

Private prison firm hit with ransomware attack

The GEO Group, the company best known for operating illegal immigration detention centres and private prisons in the US, disclosed that it suffered a ransomware attack this summer, exposing sensitive information about inmates and residents. Personal data and health information of both inmates and residents were exposed during the attack, which took place on 19 August 2020. GEO Group said that the incident impacted only a small part of its network of 123 private prisons, processing centres, immigration detention centres and mental health facilities, spanning the US, South Africa, Australia and the UK. According to ZDNet, compromised data include data for inmates at the South Bay Correctional and Rehabilitation Facility in Florida; a youth facility in Pennsylvania, and a now-closed facility in California. These details could include extremely sensitive information such as medical treatment information, in addition to details such as name, date of birth and social security number. Employee data on two corporate servers were also compromised during the attack. In a Securities Exchange Commission filing, the company states that it was able to recover its “critical operating data”, but did not disclose whether this involved paying a ransom or if it succeeded in restoring the compromised data through backup solutions. “At this time, the company is not aware of any fraud or misuse of information as a result of the incident. Based on its assessment and on the information currently known and obtained through the investigation of the incident, the company does not believe the incident will have a material impact on its business, operations or financial results,” it said. GEO Group is now sending data-breach notification letters to all individuals affected by the attack. GEO implemented several containment and remediation measures to address the incident, restore its systems and reinforce the security of its networks and information technology systems, the company said. Last week, a US federal task force – including the FBI, the Department of Health and Human Services, and the Cybersecurity and Infrastructure Security Agency – issued a warning that a serious ransomware assault against hospitals is underway. Ransomware attacks against hospitals encrypt vital data such as medical records until a ransom is paid, pressuring hospital operators to pay up in order to continue with urgent life-saving work. These ransoms are typically in the range of hundreds of thousands of dollars, but can reach into the millions. In September, all 250 facilities of Universal Health Services were targeted, forcing workers to keep records on paper and divert incoming ambulances.