UK at high risk of ‘catastrophic ransomware attack’, report says

Publication Date: 2023-12-13

Author: Sammy Gecsoyler

Section: Technology

Tags: Cybercrime, news

Article URL: https://www.theguardian.com/technology/2023/dec/13/uk-at-high-risk-of-catastrophic-ransomware-attack-report-says

The UK government is at high risk of a “catastrophic ransomware attack” that could “bring the country to a standstill” because of poor planning and a lack of investment, a parliamentary committee has warned. In a damning report, the joint committee on the national security strategy warned that the UK could face a crippling cyber-attack on its critical national infrastructure (CNI) at any moment. The National Cyber Security Centre (NCSC) describes the CNI as national assets that are essential for the functioning of society, including energy supply, water supply, transportation, health and telecommunications. Recent ransomware attacks on UK public services include an attack on the NHS last year that left patient data in the hands of cyber-attackers. In 2020, Redcar and Cleveland council fell victim to a ransomware attack and was locked out of its systems for almost three weeks. One councillor said they were told it would cost between £11m and £18m to repair the damage. The report said the government was failing to invest sufficiently to prevent large-scale cyber-attacks and criticised the Home Office, who claim the lead on ransomware as a policy issue, and former home secretary Suella Braverman, for failing to make the issue a priority. The committee said Braverman “showed no interest in [ransomware]. Clear political priority is given instead to other issues, such as illegal migration and small boats.” The committee also noted that the UK’s CNI was reliant on private, third-party IT systems that leave them vulnerable to cyber-attack. Future ransomware attacks could pose “a threat to physical security or safety of human life”, the report said, if cyber-attackers manage to sabotage CNI operations. The report also warned that “cyber-physical systems” could be intercepted, including hackers taking control of the steering and throttle of a shipping vessel – lab experiments have shown this to be achievable. The NHS was identified as a particularly vulnerable target, citing the health service’s reliance on a “vast estate of legacy infrastructure”, including “IT systems that are out of support or have reached the end of their lifecycle”. The committee noted that the health service lacks the capacity to undertake even “simple upgrades” as a result of crumbling IT services and a lack of investment. Harjinder Singh Lallie, a reader in cybersecurity at the University of Warwick, said a ransomware attack on the NHS could impact appointments, patient medical records and staff payment systems. “It could honestly be such a wide range of things. Any one of those could bring the NHS to its knees,” he said. He added that if operating systems and computer hardware were upgraded about every three to four years, overall costs and disruption would be lower. Citing the NCSC, the committee said that most ransomware groups targeting the UK are “based in and around Russia” and they benefit from “the tacit consent of the Russian State”. Ransomware groups in North Korea and Iran were also identified as targeting the UK. “The problem we have with Russia right now is because we’ve thrown our weight behind Ukraine, we’ve become a target,” said Lallie.

Margaret Beckett, chair of the joint committee, said: “The UK has the dubious distinction of being one of the world’s most cyber-attacked nations. It is clear to the committee that the government’s investment in and response to this threat are not equally world-beating, leaving us exposed to catastrophic costs and destabilising political interference. “In the likely event of a massive, catastrophic ransomware attack, the failure to rise to meet this challenge will rightly be seen as an inexcusable strategic failure.” A government spokesperson said: “The UK is well prepared to respond to cyber threats and has taken robust action to improve our cyber defences, investing £2.6bn under our cyber securitydtrategy and rolling out the first ever government-backed minimum standards for cyber security through the NCSC’s cyber essentials scheme.”