HealthManagement
Promoting Management and Leadership

‘Shielding’ Against Cyber Attacks

It is reported that Israel is planning to cover its national healthcare system with a ‘cyber defence shield’ following an increase in attacks amid the COVID-19 epidemic. Agencies elsewhere warn about the spike in cyber attacks on healthcare organisations.

You may also like: Cyber Hackers Exploit COVID-19 Crisis with Healthcare Attacks

According to The Media Line, the Israel’s plans were revealed during a Cybertech B2B online conference by *Reuven Eliyahu,* CTO and Supervisor of Health System Security & Cyber at Israel *Ministry of Health*. The new system is expected to protect healthcare facilities from cyber attacks, and will be available for free to all health organisations in Israel. This way the ministry is aiming to raise the health care sector’s resilience.

There had been “a significant increase” in attacks on healthcare organisations, said Elyiahu, since many employees had been working remotely and hackers took advantage of their less protected home systems. Moreover, he noted that many of those attacks were state-sponsored as many had been “looking to get their hands on solutions to the virus.”

In Europe, one of the latest victims to cybercriminals has been the Germany-based Fresenius Group, which provides products and services for dialysis, hospitals, and inpatient and outpatient care. As reported by KrebsOnSecurity, the attack is attributed to the relatively new Snake ransomware, that is being used to block IT systems and data of large companies in exchange for a ransom. The attack has been confirmed to the outlet by Fresenius spokesperson Matt Kuhn.

Back in April, the International Criminal Police Organisation (INTERPOL) issued a warning about “a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response.”

And on 5 May, the U.S and the U.K.’s national cybersecurity authorities (the Department of Homeland Security‘s Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Centre (NCSC), respectively) issued a joint advisory highlighting so-called ‘advanced persistent threat’ groups’ activity against organisation involved in both national and international COVID-19 responses. The advisory describes some of the methods used by the hackers and provides mitigation advice (the full text is available here).

Back in Israel, Professor Yoram Weiss, director of Hadassah Medical Center at Ein Kerem in Jerusalem, told The Media Line about hackers trying to access electronic medical records and IT infrastructure of healthcare organisations as responding to the pandemic, hospitals are creating new infrastructure for critical-care patients. The targets include, for example, telemedicine facilities, which are especially vulnerable to cyberattacks, but also more ‘traditional’ systems, such as air conditioning, which, if infiltrated, could be used to spread the coronavirus among hospital wards.

According to the CISA and NCSC’s joint alert, **o**ne of the main types of attacks is password spraying, or trying several commonly used passwords over a large number of accounts. “These attacks are successful because, for any given large set of users, there will likely be some with common passwords,” the advisory said.

Image credit: Samuel Dutler via iStock

Published on : Fri, 8 May 2020