The Cyber Attack at AIIMS Raises Many Questions

The major concern was over patient data theft, which was the most vulnerable

By NIKITA JAIN | 18 Dec 2022 10:24 AM

At All India Institute of Medical Sciences (AIIMS) things are slowly getting back to normal. However, major damage has already been done. It had affected hundreds of patients who visit the Central government run hospital daily.

On November 23, a breach was detected in the internal online information system of AIIMS. This had led the hospital to shut down most digital patient care systems, and move to manual means.

Also Read - A Tale of Two Bridges

Soon, AIIMS confirmed the attack in a media statement. It stated that data restoration and server cleaning were taking time because of the large volumes, and the number of servers that the hospital services require.

From the system of appointments to the billing and sharing of reports with patients and between departments, almost all services online at the institute were affected. Additional staff were deployed as AIIMS switched to manual mode. It went offline during the probe, even though not all servers were hit.

The major concern was over the patient data theft, which was at the most vulnerable situation. Every year, around 38 lakh patients, including top political leaders, bureaucrats and judges, get medical treatment at AIIMS. Top intelligence and anti-terror agencies, besides IT emergency teams, worked the case as all 5,000-odd computers and the servers were scanned.

The attack, many experts believe, is also due to the lack of vulnerability in digital infrastructure in healthcare institutions. Speaking more about it, Dr. Malini Saba, human rights activist and founder and chairman of Anannke Foundation said, "Cyberattacks had been able to get into the hospital's systems for a long time because they didn't have regular cybersecurity maintenance or train their employees on good online hygiene.

Also Read - Extreme Workouts Can Kill !

"According to sources' accounts, bookings, appointments, and other services were only shifted to an online system after shoddy digitisation. There were no cybersecurity measures implemented."

A ransomware is malware that encrypts data on a system, blocking users' access to that data. Hackers ask for a ransom in order to return access to that data, which in this case is said to be ₹200 crore. However, the ransomware theory has been denied by both AIIMS and the Delhi Police.

Also Read - South Asian University Students On Hunger Strike

When AIIMS was still struggling with the hack, reports that Delhi government run Safdarjung Hospital, which stands just opposite AIIMS also witnessed a cyberattack.

While AIIMS has been crippled and struggling to deal with the rush of patients, the cyber attack at Safdarjung Hospital was not as severe. Unlike AIIMS where medical records of lakhs of patients are at risk of being leaked, Safdarjung attack is unlikely to have the same concern with much of the hospital still running in manual mode.

"The hackers hit the hospital system some days ago and the server was down for one day", Safdarjung Hospital Director Dr BL Sherwal had said to the media at the time. He also informed that only some sections of the hospital were affected and the cyber attack was not of a "higher degree".

"People have said a lot about how India isn't ready for cyberattacks in general, but a trail of documents from AIIMS also shows apparent incompetence that goes along with the government's push to digitise healthcare," Dr. Saba added.

Meanwhile, at AIIMS, the hack was so severe that its repercussions are still being felt. A head nurse at AIIMS, when asked how the situation was at the hospital, on the condition of anonymity said, "There are still some functional issues that we are facing even now."

According to reports, the security professionals working at AIIMS had to check the entire system, making sure that each system on the network is malware-free. This was a major reason why so much time was taken to bring things back to normal.

"Despite multiple attacks on vital government installations over the past few months, it remains to be seen whether the number of occurrences can be brought under control. In the absence of a robust firewall surrounding data, websites remain vulnerable, and can be exploited by unscrupulous actors," Dr. Saba added.

Meanwhile, the National Investigation Agency (NIA) is investigating the "deliberate and targeted" ransomware attack on the servers of AIIMS Delhi, Minister of State for IT Rajeev Chandrasekhar has said.

"I can't comment on that as it is a subject matter of an investigation by the NIA... It is pretty clear that it is a deliberate and targeted effort... a ransomware attack on AIIMS' system... and NIA is investigating it," said Chandrasekhar.

From what is known, following the massive outage, a multi-agency investigation comprising of Indian Computer Emergency Response Team within the Ministry of Electronics and Information Technology, Delhi cybercrime special cell, Indian Cybercrime Coordination Centre, Intelligence Bureau, Central Bureau of Investigation (CBI), National Forensic Sciences University, National Critical Information Infrastructure Protection Centre and NIA, among others were launched.

Meanwhile, a report published by The Print said that the hospital's administration had raised major concerns about data and systems safety soon after AIIMS moved to a completely digitised set-up in 2016, and had flagged how lags could "have serious repercussions on patient care".

The report said that on 19 July 2016, the Delhi AIIMS, completed implementation of the e-Hospital project under the Narendra Modi government's Digital India Initiative. It became the country's first fully digital public hospital.

However, six months after full digitisation, on January 9, 2017, Dr Deepak Agrawal, from the neurosurgery department, who was then chairperson of the computerisation committee, wrote to the Union Health Ministry.

In his letter, he pointed out that the e-hospital installation by the National Informatics Centre (NIC) — the government department responsible for setting up IT infrastructure — had not been bolstered with appropriate systems for upkeep and security.

"The largest e-Hospital installation by NIC is at AIIMS, New Delhi. However, there is no database administrator, security administrator and system administrator at site for the installation, putting the whole project at risk," wrote Dr Agrawal. He added that the NIC did not have the expertise to provide any support in this regard and had asked AIIMS to recruit these experts.

Urging the health ministry to take up the matter with NIC and the Department of Electronics and Information Technology, Agrawal wrote: "[W]ithout these experts there is a major risk to e-Hospital installation at AIIMS, Delhi."

However, the incident at the hospital has only brought forward the discussion on India's Information Technology Law.

The Information Technology Act, 2000 (henceforth referred to as IT Act) is the only law that majorly deals with technology and its related issues. There are other laws like the Indian Penal Code, 1860, The Indian Evidence, 1872, The Bankers' Books Evidence Act, 1891, Prevention of Money Laundering Act, 2002 e-records maintenance policy by banks.

These legislations do not deal with technology-related laws in a wholesome manner, rather they touch upon some important aspects that are covered under the subject matter of the legislation.

According to reports, India experienced 18 million cyberattacks and 2 million threats each day during the first quarter of 2022.

Speaking about the law, Dr. Saba said, "To realise the vision of a digital healthcare ecosystem, it is essential to rethink our existing approach to cybersecurity, particularly with regards to healthcare data."

"The expansion of the digital infrastructure at the leading health institution since 1988 indicated that, given the glaring vulnerabilities, incidents similar to these cyber-attacks may have occurred a long time ago. There are difficulties such as reliance on outdated versions of system and application software, inadequate cleanliness, lack of clear ownership and skills required to manage the system properly, connectedness of key utilities, and absence of cyber security measures, to name a few," she added.

Meanwhile, social media giant Meta stated it has taken down over 40 accounts operated by Indian firm CyberRoot Risk Advisory for phishing. The accounts were allegedly involved in hacking-for-hire services, Meta said in a report. The tech giant has also taken down a network of about 900 fake accounts on Instagram and Facebook operated from China by an unknown entity.

These accounts were focused on collecting data of people in Myanmar, India, Taiwan, the US and China, including military personnel, pro-democracy activists, government employees, politicians and journalists, according to the company's Threat Report on the Surveillance-for-Hire Industry released on December 15.

"We removed a network of more than 40 accounts on Facebook and Instagram operated by an Indian firm called CyberRoot Risk Advisory Private. Rather than directly sharing malware on our apps, this group's activity manifested primarily in social engineering and phishing, often intended to trick people into giving up their credentials to various online accounts across the internet," the report stated.

According to Meta, CyberRoot used fake accounts to create fictitious personas tailored to gain trust with the people they targeted around the world and to appear more credible, these personas impersonated journalists, business executives and media personalities.

In some cases, CyberRoot also created accounts that were very identical to accounts connected to their targets like their friends and family members, with only slightly changed usernames, likely in an attempt to trick people into engaging, the report stated.

Meta said it continues to investigate and take action against spyware vendors around the world, including in China, Russia, Israel, the US and India, who targeted people in about 200 countries and territories.

The social media firm in its research has found that the global surveillance-for-hire industry continues to grow and indiscriminately target people including journalists, activists, litigants and political opposition to collect intelligence, manipulate and compromise their devices and accounts across the internet.

Interestingly, the government will release the draft Digital India bill for public consultation by the end of this month. Expected to replace the IT Act 2020, the Digital India Act, the government plans to introduce the data protection bill in the upcoming Budget session.

Speaking at the CII Global Economic Policy Summit, Chandrasekhar said, "we expect both the bills (Digital Personal Data Protection bill and Digital India Bill) to be taken to Parliament together".