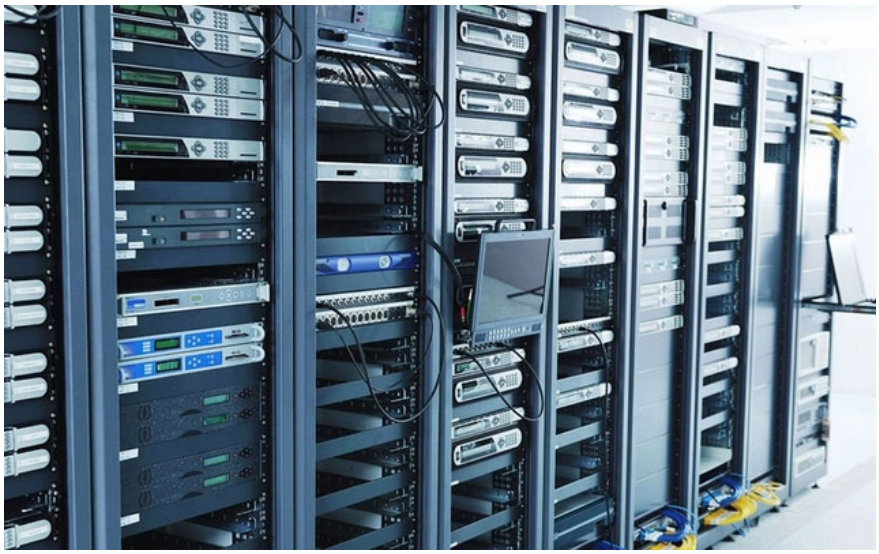
After being fired, the former employee deleted 180 of the old company's servers

Due to human negligence, NCS - an information technology company headquartered in Singapore, encountered a serious cybersecurity incident.

Kandula Nagaraju (39 years old), a former contract employee, had been a member of the 20-person team since November 2021 but due to ineffective work, his contract was terminated in October 2022 and had his last working day. The same is November 16, 2022.



Due to "human negligence", when Kandula left the company, his access to NCS's systems was not immediately blocked.

Taking advantage of this loophole, Kandula used his personal laptop 6 times to illegally access NCS's system from India - where he returned after being fired, from January 6 to September 1. January 17, 2023. This system includes about 180 virtual servers and does not store sensitive information.

In February 2023, Kandula returned to work for a new company in Singapore. Here, he continued to use the Wi-Fi network of a former colleague at NCS to illegally access the company's system on February 23, 2023.

After repeatedly accessing NCS's QA system, Kandula ran malicious code he wrote to delete 180 virtual servers, causing NCS a loss of 917,832 SGD.

Kandula's crime was discovered. In court, Kandula admitted that he knew that accessing the system after quitting his job was illegal.

After this incident, NCS has strict procedures and control measures in place.

The incident once again raises the alarm about cybersecurity vulnerabilities in businesses, in which strict control of system access rights after employees leave needs to be implemented quickly to prevent attacks. risks.