

US subsidiary of meat-packing giant JBS hit by cyberattack

June 1 2021



JBS is a sprawling meat supplier with operations in the United States, Australia, Canada, Europe, Mexico, New Zealand and Britain.

The American subsidiary of the world's largest meat processing companies said Monday it had been hacked, paralyzing some of its

operations and impacting thousands of workers in Australia.

The intrusion was detected Sunday, forcing one of the leading producers of beef and pork in the United States to suspend affected systems, and call in its IT staff and third-party experts to deal with the breach.

"JBS USA determined that it was the target of an organized [cybersecurity](#) attack, affecting some of the servers supporting its North American and Australian IT systems," the unit said in a statement.

The hack comes less than a month after a major cyberattack shut down the Colonial Pipeline network, which transports about 45 percent of fuel consumed on the east coast of the United States.

Brazil-based JBS is a sprawling meat supplier with operations in the United States, Australia, Canada, Europe, Mexico, New Zealand and Britain.

The company's Australian facilities were said to have been paralyzed by the attack, with up to 10,000 meat workers being sent home without pay, according to a union representative.

"It's affecting JBS processing facilities around (Australia)," AMIEU Queensland branch secretary Matt Journeaux told AFP. "They have stood down workers across JBS operations."

Journeaux said there was no word yet from the company on when operations will resume.

JBS Foods is one of Australia's largest meat and food processing companies and plays a key role in the country's [agriculture sector](#), making \$2.4 billion in livestock purchases each year.

In a statement to AFP, Australian Agriculture Minister David Littleproud said he was "aware of reports" of the attack but declined to comment "until further details are available."

JBS USA said it was "not aware of any evidence at this time that any customer, supplier or employee data has been compromised or misused," but the attack may cause delays for customers and suppliers.

It said its backup servers were not affected.

Cybersecurity vulnerabilities

Colonial's multi-day shutdown in May sparked panic buying in some eastern states, and ended when the company paid \$4.4 million in ransom to the hackers.

The demonstrated online vulnerabilities of US pipelines led the [federal government](#) last week to impose cybersecurity requirements on petroleum pipelines for the first time.

The new rules, imposed by the Department of Homeland Security, require pipeline operators to designate a cybersecurity coordinator who must be available at all times, and report confirmed incidences to the agency's Cybersecurity and Infrastructure Security Agency.

Pipeline owners will also be required to review their procedures and identify cybersecurity gaps and ways to fix them, with the results reported to the department within 30 days.

"The cybersecurity landscape is constantly evolving and we must adapt to address new and emerging threats," Homeland Security Secretary Alejandro Mayorkas said in a statement Thursday.

© 2021 AFP

Citation: US subsidiary of meat-packing giant JBS hit by cyberattack (2021, June 1) retrieved 8 April 2024 from

<https://techxplore.com/news/2021-06-subsiidiary-meat-packing-giant-jbs-cyberattack.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.