Australia ports firm fights to restore operations after cyber incident

November 12 2023

The 'cyber securiry incident' has affected operations at ports in Sydney, Melbourne, Brisbane and Fremantle.

Ports operator DP World said Sunday it had made "significant strides" towards resuming normal freight trade at major gateways into Australia,

which have been crippled for two days by a cyber incident.

Government agencies held crisis talks over the weekend in response to what Home Affairs and Cyber Security Minister Clare O'Neil described as a "serious and ongoing" breach that has disrupted operations at key ports.

"DP World manages almost 40 percent of the goods flowing in and out of our country," she added in a post on X.

The port operator halted internet connectivity at its terminals in Sydney, Melbourne, Brisbane and Fremantle on Friday to prevent "any ongoing unauthorized access" to its network, a company spokesperson said.

The disruption has not prevented containers from being taken off vessels but trucks needed to transport them have not been able to drive in or out of the terminals, DP World senior director Blake Tierney said.

In a statement, Tierney said the company had made "significant strides" working with cybersecurity experts and was testing key systems "crucial for the resumption of regular freight movement".

The company was seeking to restore normal operations "as quickly and safely as possible", he said, and was investigating "the nature of data access and data theft".

"DP World Australia is working hard to assess whether any personal information has been impacted," Tierney added.

Australian Federal Police have said they are investigating the incident.

National Cyber Security Coordinator Darren Goldie said on X on Sunday that the company has told the government any disruption to port

operations is "likely to be a number of days, rather than weeks".

"DP World's IT system remains disconnected from the internet, significantly impacting their operations," he added.

Despite the disruption, the port operator is able to "access sensitive freight if necessary -– for example, in a medical emergency," Goldie also said.

Lucrative target

After emergency meetings on Saturday, Goldie again convened the National Coordination Mechanism on Sunday with representatives from government, maritime and logistics sectors to manage the government's response.

Australia's National Emergency Management Agency also attended the talks.

Goldie, an air marshal in the Royal Australian Air Force, was appointed the inaugural national coordinator last July in response to several cyber attacks.

Cybersecurity experts have said inadequate safeguards and the stockpiling of sensitive customer information have made Australia a lucrative target for hackers.

Medibank, Australia's largest private health insurer, said in November 2022 that hackers had accessed the data of 9.7 million current and former customers, including medical records related to drug abuse and pregnancy terminations.

Just two months earlier, telecom company Optus fell prey to a data

breach of similar scale in which the personal details of up to 9.8 million people were accessed.

Those two incidents were among the largest data breaches in Australian history.

Optus, Australia's second-largest phone provider, apologized to its more than 10 million customers last week over a "technical network outage" that crashed electronic payments, disrupted phone lines used by emergency services and stopped people accessing government services.

The Australian government has launched an investigation into that unexplained glitch, although it has not been described as a cyber attack.

There were 76,000 cybercrimes reported to the Australian Cyber Security Centre last year, although experts warn many more go unreported.

Citation: Australia ports firm fights to restore operations after cyber incident (2023, November 12) retrieved 8 May 2024 from https://techxplore.com/news/2023-11-australia-ports-firm-cyber-incident.html