

Biden is boosting cybersecurity at US ports, where online attacks can be more ravaging than storms

February 21 2024, by Colleen Long

President Joe Biden on Wednesday signed an [executive order and created a federal rule](#) aimed at better securing the nation's ports from potential cyberattacks.

The administration is outlining a set of cybersecurity regulations that port operators must comply with across the country, not unlike standardized safety regulations that seek to prevent injury or damage to people and infrastructure.

"We want to ensure there are similar requirements for cyber, when a cyberattack can cause just as much if not more damage than a storm or another physical threat," said Anne Neuberger, deputy national security adviser at the White House.

Nationwide, ports employ roughly 31 million people and contribute \$5.4 trillion to the economy, and could be left vulnerable to a ransomware or other brand of cyberattack, Neuberger said. The standardized set of requirements is designed to help protect against that.

The new requirements are part of the federal government's focus on modernizing how critical infrastructure like power grids, ports and pipelines are protected as they are increasingly managed and controlled online, often remotely. There is no set of nationwide standards that govern how operators should protect against potential attacks online.

The threat continues to grow. Hostile activity in cyberspace—from spying to the planting of malware to infect and disrupt a country's infrastructure—has become a hallmark of modern geopolitical rivalry.

For example, in 2021, the operator of the nation's largest fuel pipeline had to temporarily halt operations after it fell victim to a ransomware attack in which hackers hold a victim's data or device hostage in exchange for money. The company, Colonial Pipeline, paid \$4.4 million to a Russia-based hacker group, though Justice Department officials later recovered much of the money.

Ports, too, are vulnerable. In Australia last year, a cyber incident forced one of the country's largest port operators to suspend operations for three days.

In the U.S., roughly 80% of the giant cranes used to lift and haul cargo off ships onto U.S. docks come from China, and are controlled remotely, said Admiral John Vann, commander of the U.S. Coast Guard's cyber command. That leaves them vulnerable to attack, he said.

Late last month, U.S. officials said they had disrupted a state-backed Chinese effort to plant malware that could be used to damage civilian infrastructure. Vann said this type of potential attack was a concern as officials pushed for new standards, but they are also worried about the possibility for criminal activity.

The new standards, which will be subject to a public comment period, will be required for any port operator and there will be enforcement actions for failing to comply with the standards, though the officials did not outline them. They require port operators to notify authorities when they have been victimized by a cyberattack. The actions also give the Coast Guard, which regulates the nation's ports, the ability to respond to cyberattacks.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Biden is boosting cybersecurity at US ports, where online attacks can be more ravaging than storms (2024, February 21) retrieved 4 May 2024 from <https://techxplore.com/news/2024-02-biden-boosting-cybersecurity-ports-online.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.