Pipeline Hack Points to Growing Cybersecurity Risk for Energy System

The New York Times, May 13, 2021

The audacious ransomware attack that shut down a major fuel pipeline and sent Americans scrambling for gasoline in the Southeast this week was not the first time hackers have disrupted America's aging, vulnerable energy infrastructure. And it's unlikely to be the last.

Across the globe, cyberattackers are increasingly taking aim at the energy systems that underpin modern society. A February report from IBM found that the energy industry was the third most targeted sector for such attacks in 2020, behind only finance and manufacturing. That was up from ninth place in 2019.

"This should be a wake-up call," said Jonathon Monken, a principal at the energy consulting firm Converge Strategies. "When you look at what's most likely to cause disruptions to energy companies today, I think you have to put cybersecurity risks at the top."

Despite years of warnings, America's vast network of pipelines, electric grids and power plants remains acutely vulnerable to cyberattacks with the potential to disrupt energy supplies for millions of people. Dealing with those risks, analysts said, will pose a major challenge for the Biden administration as it seeks hundreds of billions of dollars to modernize the nation's energy infrastructure and transition to cleaner sources of energy to address climate change.

Regulators are increasingly poised to step in. On Monday, Richard Glick, the chairman of the Federal Energy Regulatory Commission, said it was time to establish mandatory cybersecurity standards for the nation's nearly 3 million miles of oil and gas pipelines, similar to those currently found in the electricity sector.

"Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors," Mr. Glick said in a statement.

And it's not just pipelines. As electric grid operators harness a growing array of digital technologies to help manage the flow of power and cut planet-warming emissions — such as smart thermostats, or far-flung yet interconnected networks of solar arrays — hackers may find new entry points to exploit.

The shutdown on Friday of the Colonial Pipeline, which stretches 5,500 miles from Texas to New Jersey and transports 45 percent of the East Coast's fuel supplies, illustrates how devastating such attacks can be.

On Saturday, Colonial acknowledged that its corporate computer systems had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom. The company said that it had shut down the pipeline as a precaution, apparently for fear that the hackers might have obtained information that would enable them to attack parts of the pipeline itself.

While Colonial has yet to explain exactly what triggered the pipeline shutdown, experts said there were plenty of vulnerabilities lurking throughout America's energy infrastructure.

In the past, energy companies typically kept the operational systems that run pipelines or power plants disconnected, or "air gapped," from the broader internet, which meant that hackers could not easily gain access to the most critical infrastructure. But increasingly that's no longer the case, as companies install more sophisticated monitoring and diagnostics software that help them operate these systems more efficiently. That potentially creates new cybersecurity risks.

Energy companies may never be able to defend themselves against every single potential cyberattack out there, experts said. Instead, businesses and policymakers will need to design broader energy systems that are resilient to attacks and potential shutdowns, by, for instance, building in more redundancies or overrides.

"It's an old saying in cybersecurity: The people working defense have to be right 100 percent of the time, while the attackers only have to be right once," Mr. Monken said. "That means we have to think a lot harder about contingencies when those defenses fail."