Updates
March 07, 2023
FERC Establishes New Monitoring Requirements for Bulk Electric Systems

In late January, the Federal Energy Regulatory Commission (FERC) published a final rule directing the North American Electric Reliability Corporation (NERC) to develop and submit modified reliability standards for internal network security monitoring within networked environments that fall under the Critical Infrastructure Protection (CIP) set of requirements. FERC identified a potential security gap under current reliability standards that focus on perimeter monitoring and security, leaving CIP-networked assets vulnerable to attacks that bypass the network perimeter. Emphasizing perimeter security without addressing internal security—or, ignoring the enemy after it has come through the castle wall—is a common cybersecurity error.

Under the final rule, the new standards will apply to CIP-networked environments for all high-impact bulk electric systems, as well as medium-impact systems with external roundtable connectivity. The rule generally requires such entities to bolster their cybersecurity capabilities across three areas:

- Identifying baseline network traffic patterns to enable anomaly detection.
- Implementing technologies that can monitor and detect unauthorized behavior and other anomalies within a trusted network (e.g., unusual connections, devices, traffic patterns, or software).
- Collecting data, including logs of network traffic, which are necessary to more confidently analyze potential threats and prevent attackers from easily covering their tracks.

According to FERC, by supporting timely detection and effective response, internal network security monitoring can help reduce the surface area of an attack even if attackers successfully penetrate the network. FERC also directs NERC to perform a study on the cybersecurity of bulk electric systems (BES) that are not subject to the final rule (i.e., low-impact systems and medium-impact systems that lack external roundtable connectivity).

While the existing Critical Infrastructure Protection standards require BES operators to monitor the perimeter of their networked environment, no such guidelines exist regarding activity within the trusted zone. The absence of such standards can create a critical blind spot with respect to threat detection and response for attacks that

succeed in bypassing these perimeter-based controls, whether due to stolen credentials, supply chain compromise, or insider threat.

FERC's final rule on the matter narrows the scope of its prior notice of proposed rulemaking, which called for such standards to apply to all high-impact systems and medium-impact bulk electric systems. In justifying the change, FERC pointed to a number of comments highlighting how a broader-based rule would exacerbate challenges to implementation, particularly in light of ongoing supply chain shortages and the dearth of skilled cybersecurity professionals (who are already overworked in the face of an escalating cyber threat landscape and increased regulatory attention to cybersecurity across the Biden Administration). FERC's decision affirms that a narrower rule can, itself, offer cybersecurity benefits by focusing efforts on the highest-impact systems and accelerating the timeline by which implementation is feasible.

A Sign of Larger Shifts

While the number of entities that the rule directly affects may be smaller, the rule underscores several larger trends in the Biden Administration's approach to cybersecurity.

First, it recognizes the imperative of improving the cybersecurity and resiliency of critical infrastructure systems, many of which are privately owned and operated but nonetheless fundamental to U.S. national security. Just last week, in its National Cybersecurity Strategy, the Biden Administration recognized defending critical infrastructure as the first of five high-level cybersecurity priorities.

Second, it recognizes that there is no "silver bullet" when it comes to cybersecurity and that defenders must be ready to adapt their approach to stay ahead of attackers. The requirements for internal network security monitoring cannot be achieved through a single technology or procedural change and must include the embrace of zero trust principles across multiple security tools and operational practices. The same shift underpins the Biden Administration's Executive Order 14028 on Improving the Nation's Cybersecurity, which calls upon all federal agencies to make long-term investments in zero trust tools and architectures, where many had previously relied upon perimeter-based approaches to ensuring security.

Third, it reflects the increased scrutiny of software supply chain security. The software supply chain is a critical vector through which attackers can penetrate closed systems. In this vein, FERC highlights the SolarWinds attack, in which the compromise of widely deployed software allowed foreign threat actors to not only compromise trusted networks but [also to] move laterally across a large number of public and private networks thereafter. Effective network monitoring systems could, at least in theory, enable faster detection of threats and reduce their spread, as compared to the massive impact of the SolarWinds compromise.

Accordingly, entities in the energy sector and beyond should view the new FERC rule as another signal of the direction in which U.S. cybersecurity policy is heading. Critical infrastructure companies should expect more numerous, more comprehensive, and more prescriptive security rules. Given the priority placed on supply chain security, the requirements placed upon operators of high- and medium-impact systems may well trickle down to downstream providers through service provider and other agreements. They fit within a larger pattern of parallel efforts to improve critical infrastructure security. As both Congress and Executive Agencies weigh how to identify and regulate the cybersecurity privately owned and operated critical infrastructure providers, Sector Risk Management Agencies and other policymakers are likely to borrow from one another in the development of critical infrastructure security frameworks.

What's Next?

FERC's final rule will be effective April 10, 2023. NERC's revised reliability standards are due to be filed with FERC for approval on July 10, 2024 (15 months after the effective date of the final rule), and NERC's report on its study of low-impact systems and medium-impact systems that lack external roundtable connectivity is due to be filed with FERC by January 19, 2024 (12 months after issuance of the final rule).

Authors

Explore more in

Energy Infrastructure & Clean Technology

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law