crowell moring

CLIENT ALERT

NERC Issues "Lesson Learned" From a Cyberattack on an Electricity Control Center

Sep.13.2019

On September 4, the North American Electric Reliability Corporation (NERC) issued a "Lessons Learned" from a March 5, 2019 cyberattack on a low-impact grid control center and several small power generation sites in the western United States. NERC's assessment provides guidance to NERC-registered entities on this incident, which was previously reported to the U.S. Department of Energy.

The cyber disruption is described as "brief (i.e. less than five minutes) outages of internet-facing firewalls that controlled communications between the control center and multiple remote generation sites and between equipment on these sites." These outages continued over a 10-hour period. NERC concludes that these outages "had no impact to generation" and notes that the targeted NERC-registered entity mitigated the immediate risks and then undertook corrective actions "to reduce the likelihood of an event with a similar cause from happening again."

NERC's release details "good cyber security policies and procedures." This guidance is intended "to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system," and invites interested parties both to comment on the guidance document, and to contact NERC or the Western Electric Coordinating Council (WECC) directly.

Among other things, NERC underscores the need to utilize technical actions along with effective policies, including the need to

- timely know what exploitable vulnerabilities are on a network,
- closely monitor vendor firmware updates and patch releases, and
- implement appropriate patch management practices to address known vulnerabilities.

As NERC recognizes, an important lesson from this event is that the victim entity had not identified the vulnerability on its network before the attack and, thus, had not implemented the firmware update available from the firewall vendor that would have closed it–a fact pattern that is too frequently at the heart of cybersecurity incidents.

Additional technical concepts highlighted by NERC include

- reducing and controlling the attack surface by having as few internet-facing devices as possible,
- implementing layered defenses (e.g., screening router, virtual private network terminator and a firewall) rather than relying on only a firewall, and
- segmenting networks (i.e., restricting lateral communication to necessary and expected network traffic).

NERC also identifies useful third party resources, such as external vulnerability scanning (through DHS or security vendors), vulnerability tracking sites, and participation in the Electricity Information Sharing and Analysis Center (E-ISAC).

The March 5 event qualifies as what is becoming a flock of canaries in the cybersecurity coal mine. NERC, together with the multiple other federal agencies partly responsible in this space (including DOE, FERC, and WECC) are necessarily balancing the need for useful disclosure to the industry against the perils of providing road maps to potential bad actors looking for disruptive opportunities. Owners of critical energy infrastructure in the electric power sector are advised to review carefully NERC's guidance, to benchmark NERC's recommendations against their own cybersecurity measures, to rigorously road test those measures in simulated exercises, and to engage with their public governing agencies (e.g., NERC, DHS, DOE) and private groups and vendors (e.g., E-ISAC, supply chain, /vendors) to timely share cyber threat information and best practices.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Deborah A. Carpentier
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2857
Email: dcarpentier@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com