NATIONAL RENEWABLE ENERGY LABORATORY

COMPANY

United States
National Renewable
Energy Laboratory
www.nrel.gov

INDUSTRY

Energy/Utility

VIASAT SERVICES

Cybersecurity Vulnerability Assessment, Penetration Testing, and Secure Network Implementation

CASE STUDY

Cybersecurity Best Practices for Distributed Energy Grids

United States National Energy Laboratory (NREL) develops clean energy and energy efficiency technologies and practices, advances related to science and engineering, and provides knowledge and innovations to integrate energy systems at all scales.

The Challenge

The introduction of new technologies like smart meters and renewable energy resources has required the energy grid to move from a centralized topology to one that is highly distributed. As a result, new security vulnerabilities have surfaced. Until now, industry collaboration on how to address the cybersecurity and resilience requirements of distribution grid management (DGM), the part of the grid that carries power from substations to homes and businesses, has been very limited due to varying regulatory environments, strict NDAs, and budget constraints. To thoroughly test the effectiveness of common security controls and establish baseline standards that could be shared throughout the industry, NREL created an end-to-end DGM system test bed leveraging a bottom-up network security approach. Provided with real energy system use cases, Viasat was tasked with penetrating the test bed security and helping remediate critical vulnerabilities.

The Solution

1 Gather Information
2 Map Out Threats
3 Analyze Vulnerabilities
4 Exploit Vulnerabilities
5 Detailed Report/ Remediate

Throughout the course of a few weeks, Viasat leveraged the above process to thoroughly test, assess, and help improve the DGM system cybersecurity.

During the first phase, IT security proved strong, but a misconfigured management port on the operational technology (OT) network created a significant vulnerability. Viasat was able to penetrate one of the cybersecurity technologies through a misconfigured management port, enabling them to assume administrator rights and ultimately disrupt the entire DGM functionality by simulating a Distributed Denial of Service (DDoS) attack through the compromised device.

Prior to the second phase of testing, Viasat helped NREL re-build the test bed based on a secure IP addressing scheme that reinforced the existing layered defense approach. The additional system hardening successfully protected the test bed system, as no vulnerabilities were uncovered in the second round of penetration testing. NREL's DGM 2.0 test bed system proved capable of withstanding multiple exploits throughout successive layers of security, keeping critical energy control system assets protected.

Benefits

With support from Viasat and a handful of other partners, NREL has empirically validated an end-to-end cybersecurity architecture for distributed grid management. Individual energy utilities can use this architecture to improve distribution system resiliency and better protect against internal and external cybersecurity threats of any level of severity.

> ***"The Viasat project team demonstrated superior skills in network design implementation, penetration testing, and technical report writing. The strong collaborative spirit of its experts enabled the timely completion of a high-value project on time and on budget."***
>
> *—Dr. Erfan Ibrahim, Center Director for Cyber-Physical Systems Security & Resilience at NREL*

CONTACT

SALES
TEL +1 760 476 4755   **EMAIL** insidesales@viasat.com   **WEB** www.viasat.com/cyber-services