SWISSGRID
POWERS UP CYBERSECURITY

by Jenny Mangelsdorf

As a strategic transmission player in Europe's power grid network, Swissgrid needs to meet the most robust cybersecurity standards. The company worked with CSC to assess its operations and benchmark them against U.S. critical infrastructure protection standards.

"Every company today is asking the same question: 'How safe are we?'" says Rajesh Nair, Swissgrid head of strategy and architecture. "That's like asking a person, 'How good are you?' You can't answer that, but if you take a path using something that you can benchmark against, then you know where you stand and have something to base your investments on."

Challenge:
- Evaluate infrastructure against U.S. cybersecurity standards
- Find processes to mitigate risks
- Determine the impact of smart technologies on the grid

Solution:
- Measure infrastructure against NERC-CIP standard
- Analyze risks, using tools from U.S. Department of Homeland Security
- Recommend ways to mitigate cybersecurity risk

Results:
- Swissgrid now has a better-fortified infrastructure
- Semi-annual cybersecurity audits are planned
- Swissgrid is implementing the CSC recommendations

Switzerland has played a central role in Europe's electricity grid for more than 50 years. In 2006, Swissgrid began taking responsibility for the country's transmission grid following the European Union's liberalization of electricity markets. In 2013, Swissgrid will have complete control of the country's 6,700-kilometer high-voltage grid network.

Swissgrid ensures that power is available within the country. It also coordinates the movement of electricity and manages grid use when energy suppliers in other countries use the grid to move power across Europe to other countries.

"There's an enormous amount of power coordination going on that Switzerland manages," says Hank Hensel, CSC technical security expert. "If its grid were to go down, lights could go out in another country."

Protecting infrastructure stability

Besides the typical intricacies of managing intracountry power transfer and flow, cyberattacks add an increasing challenge to maintaining grid stability.

In a 2011 survey by CSC partner McAfee and the Center for Strategic and International Studies, 40% of 200 IT security executives from critical electricity infrastructure enterprises in 14 countries reported that their industry's vulnerability had increased.

More than 40 percent of these executives said they expect a major cyberattack within the next year that will cause severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company.

To prepare for these realities, Swissgrid looked to the North American Electric Reliability Corp. (NERC) U.S.-mandated Critical Infrastructure Protection (CIP) standard for the country's bulk-power system.

"NERC-CIP, of which v4 should be approved this year, is the only full standard that addresses high-voltage transmission and Supervisory Control and Data Acquisition (SCADA) systems used for critical infrastructure," says Meir Shargal, CSC utilities strategy leader.

Swissgrid chose CSC to benchmark it against the standard because of our NERC-CIP knowledge and expertise combined with our understanding of how to apply this to utilities.

The company also selected CSC because of our history in working with international energy companies to meet U.S. Department of Energy regulatory requirements for classified and unclassified industrial control networks, as well as our work in helping define and review cybersecurity infrastructure standards.

Benchmarking cybersecurity

CSC provided consulting services, subject matter experts, and U.S. and international regulatory expertise to benchmark Swissgrid's security standards, procedures and processes against NERC-CIP. CSC experts evaluated the company's security measures while conducting a risk and gap analysis using the U.S. Department of Homeland Security's (DHS) Cyber Security Evaluation Tool.

> "Every company today is asking the same question: 'How safe are we?'"
>
> - Rajesh Nair, Swissgrid head of strategy and architecture

"We also used DHS tools that are set up explicitly to assess a company's posture for NERC-CIP itself," Hensel says. "At the end we gave Swissgrid a baseline of where it is relative to the standard and a road map it can follow to ensure that it has robust cybersecurity in place for the future."

Today Swissgrid is acting on CSC's recommendations and implementing processes and initiatives to mitigate risks identified during the benchmark. It also plans to perform a bi-yearly NERC-CIP audit to track improvements and ensure that its security remains robust.

"In the future, as smart grid technologies and other devices with IP addresses increasingly link to networks, utilities will have to securely manage those connection points," Shargal says. "By thinking about this now, Swissgrid won't have to redesign its security infrastructure as its connections, vulnerabilities and risks increase." ■

Learn more at **www.csc.com/cybersecurity**.

JENNY MANGELSDORF is a writer for CSC's digital marketing team.