NEWS

22

NUMBER OF MINUTES IT TOOK A CYBERDEFENSE TEAM TO BREAK INTO A NORTHWEST U.S. UTILITY

ARUNAS KLUPSAS/GETTY IMAGES

CYBERSECURITY AT U.S. UTILITIES DUE FOR AN UPGRADE

Tech to detect intrusions into industrial control systems will be mandatory

The hackers who unplugged 225,000 people from the Ukrainian electricity grid in December—the first confirmed cyber-takedown of a power system—have lent credence to calls by cybersecurity experts for greater vigilance by utilities. "It's really brought the whole thing to a head and made people aware that this isn't just chatter about the sky falling," says Eric Byres, a security consultant who commercialized one of the first firewalls for industrial control systems.

Experts such as Byres say that what's needed are active security measures that detect and thwart attacks, as opposed to what the utilities have been doing—simply trying to wall off their control systems. The same message is now coming from the North American Electric Reliability Corp. (NERC), which sets binding standards for power grids in its region. NERC's newly upgraded cybersecurity codes require network monitoring and other active defenses and begin to go into effect in July. Will they be enough to stop an attack »

like the one in Ukraine? It depends on how quickly and thoroughly utilities act, experts say.

The Ukraine attack has been particularly instructive: Reports by the affected utilities, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and by independent researchers reveal that it was sustained and multipronged. "These attackers are not blindly hacking away. They're doing their research," says Byres. And the attack had long-lasting effects. Two months after the blackouts began, the affected regional utilities, or *oblenergos*, were still limping along, according to ICS-CERT's late-February bulletin: "While power has been restored, all the impacted oblenergos continue to run under constrained operations." (See timeline below.)

North American cybersecurity experts say the U.S. power grid is not well protected against the kind of campaign that hit Ukraine. "Everything about this attack was repeatable in the United States," according to Robert Lee, a former cyberwarfare operations officer for the U.S. Air Force who went to Ukraine to independently assess the December attack. "While their security wasn't awesome, it definitely wasn't below the [industry] standards," says Lee, who is the CEO of Dragos Security, based in San Antonio, which develops cybersecurity tools for SCADA (supervisory control and data acquisition) systems.

NERC's Critical Infrastructure Protection standard (NERC-CIP), in place since 2006, has primarily demanded creation of an "electronic security perimeter"—a mix of physical and electronic security measures designed to keep bad guys from accessing utility SCADA systems. This perimeter is meant to surround key transmission substations, generating plants, and other sensitive equipment. Compliance has assured a "very basic" level of security, according to Chris Sistrunk, senior consultant for the cybersecurity firm Mandiant Consulting Services, in Alexandria, Va., and a former SCADA engineer for the New Orleans-based utility Entergy.

But relying solely on perimeter protection is problematic: Should an attacker break through, SCADA systems are left vulnerable. Sistrunk points to the fact that many substations' SCADA equipment does not support authentication and encryption. A hacker who breaks into them can access utility control centers or fool operators with misleading readings. "An attacker can simply replay, modify, and spoof the traffic to SCADA devices," says Sistrunk.

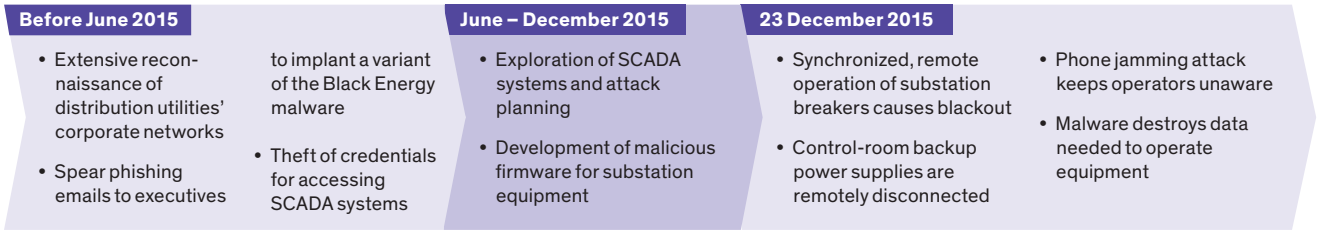
What's more, the perimeter needing protection is fast expanding. Utilities are making their grids smarter by attaching millions of interactive devices to their IT and SCADA networks—including smart meters, electric car chargers, rooftop solar installations, and other intelligent devices on customer premises that are expected to help utilities manage power flows in the future [see "How Rooftop Solar Can Stabilize the Grid," *IEEE Spectrum*, February 2015]. In the wrong hands these devices could, in theory, also be manipulated to destabilize power grids.

Cybersecurity experts advocate a more active approach, based on detecting and thwarting intrusion. This scheme is several decades old for IT systems, but it has only recently become commercially available for SCADA systems—especially for those using the DNP3 communications protocol that is most common on North America's power grids.

In 2008, Byres released one of the first SCADA traffic checkers, the Tofino Industrial Security Solution, developed in 2005 while he was at the British Columbia Institute of Technology's Critical Infrastructure Security Centre, in Burnaby. The Tofino firewall, later acquired by the St. Louis-based networking firm Belden, checks the validity of every SCADA data packet crossing a network. "It's not just looking at what protocols are allowed but what's the exact functionality of that message," explains Byres. "For example, will it just read the status of a protection relay, or completely reprogram the device? Obviously, there is a big difference between those two actions when it comes to security."

Applying Byres's approach to power-grid SCADA systems required further work, however, thanks to the complex, binary messages that make up the DNP3 protocol. A technical breakthrough came in 2012 with the coverage of DNP3 by an extension of Snort, an open-source intrusion-detection

The Attack on Ukraine's Grid



Source: ICS-CERT, SANS Institute

system. Since 2014, several DNP3-capable commercial packages have been released, and Belden was preparing a DNP3-capable Tofino firewall as *Spectrum* went to press in April.

Visualization tools designed to highlight anomalies in SCADA traffic patterns are another recent innovation. These include systems developed by Lee's firm, Dragos Security, and NexDefense, an Atlanta-based spinoff of Idaho National Laboratory, in Idaho Falls. Lee says that monitoring and visualization tools are not panaceas guaranteeing security but rather a "starting point" for identifying and countering intrusions.

To date, uptake by utilities is slow. Sistrunk says he knows of only four or five leading utilities that widely deploy SCADA monitoring and intrusion detection. Only one has presented research on its use of SCADA monitoring, and that utility requested that *Spectrum* withhold its name, arguing that such publication would "paint a target" on its networks.

The latest updates to NERC-CIP should accelerate deployment. They add, for the first time, mandates for continuous network monitoring and deployment of network defenses to detect or block malware and malicious communications. The broader standard will help, says Sistrunk, if utilities do more than the bare minimum required to check off a box on a compliance list. As he puts it, "Monitoring will increase. However, monitoring for compliance and monitoring for security aren't exactly the same thing."

Doug Wylie, a NexDefense vice president, expressed similar concerns in March after utility trade groups successfully petitioned to delay the new mandates' start date from April to July. The delay, wrote Wylie on NexDefense's blog, "underscores the need for the energy industry to create a security culture that prioritizes the mitigation of dangerous and frequent cyber threats."

—PETER FAIRLEY

KIM KULISH/CORBIS

WHEN WILL GOOGLE'S SELF-DRIVING CAR *REALLY* BE READY?

It depends on where you live and what you mean by "ready"

If you're one of the millions of people pining to own a Google self-driving car, you'd better make yourself comfortable, because you may be in for a much longer wait than you ever expected. Not only that: There's a distinct chance that once you get behind the wheel of the first commercial version of the Google car, it may not be able to take you where you need to go.

SOON FOR SOME: Google's vision of a car that can take you anywhere might take longer to achieve, depending on where your "anywhere" is.

In 2011, soon after Google first told the world about the robocars it had secretly been developing, it promised that the vehicles would be able to "drive anywhere a car can legally drive." The company's time frame for delivering the technology was generally understood to be in the neighborhood of five years. For example, in a 2014 *Wall Street Journal* article, project director Chris Urmson was quoted as saying he was hoping "to field a fully autonomous car" by the end of the decade.

But in a speech he gave in March at South by Southwest, in Austin, Texas, Urmson for the first time told a different story about both the delivery date and capabilities of Google's first self-driving cars.

Not only might they take much longer to arrive than the company has ever indicated—as long as 30 years, said Urmson—but the early commercial versions might well be limited to certain geographies and weather conditions. Self-driving cars are much easier to engineer for sunny weather and wide-open roads, and Urmson suggested the cars might be sold in those markets first.

Urmson put it this way in his speech: "How quickly can we get this into people's hands? If you read the papers, you see maybe it's three years, maybe it's 30 years. And I am here to tell you that honestly, it's a bit of both."

He went on to say, "This technology is almost certainly going to come out incrementally. We imagine we are going to find places where the weather is good, where the roads are easy to drive—the technology might come there first. And then once we have confidence with that, we will move to more challenging locations."

In an interview, a Google spokesman agreed that Urmson was describing some aspects of the project differently than the com-