

Slammer worm crashed Ohio nuke plant network

Kevin Poulsen, SecurityFocus 2003-08-19

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

The breach did not pose a safety hazard. The troubled plant had been offline since February, 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common, and is permitted by federal safety regulations.

The Davis-Besse plant is operated by FirstEnergy Corp., the Ohio utility company that's become the focus of an investigation into the northeastern U.S. blackout last week.

The incident at the plant is described in an April e-mail to the Nuclear Regulatory Commission (NRC) from FirstEnergy, and in a similarly-worded March safety advisory distributed privately throughout the industry over the "Nuclear Network," an information-sharing program run by the Institute of Nuclear Power Operations. The March advisory was issued to "alert the industry to consequences of Internet Worms and Viruses on Plant Computer Systems," according to the text.

The reports paint a sobering picture of cybersecurity at FirstEnergy.

The Slammer worm entered the Davis-Besse plant through a circuitous route. It began by penetrating the unsecured network of an unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and Davis-Besse's corporate network. The T1 line, investigators later found, was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread.

"This is in essence a backdoor from the Internet to the Corporate internal network that was not monitored by Corporate personnel," reads the April NRC filing by FirstEnergy's Dale Wuokko. "[S]ome people in Corporate's Network Services department were aware of this T1 connection and some were not."

Users noticed slow performance on Davis-Besse's business network at 9:00 a.m., Saturday, January 25th, at the same time Slammer began hitting networks around the world. From the business network, the worm spread to the plant network, where it found purchase in at least one unpatched Windows server. According to the reports, plant computer engineers hadn't installed the patch for the MS-SQL vulnerability that Slammer exploited. In fact, they didn't know there was a patch, which Microsoft released six months before Slammer struck.

Operators Burdened

By 4:00 p.m., power plant workers noticed a slowdown on the plant network. At 4:50 p.m., the congestion created by the worm's scanning crashed the plant's computerized display panel, called the Safety Parameter Display System.

An SPDS monitors the most crucial safety indicators at a plant, like coolant systems, core temperature sensors, and external radiation sensors. Many of those continue to require careful monitoring even while a plant is offline, says one expert. An SPDS outage lasting eight hours or more requires that the NRC be notified.

At 5:13 p.m., another, less critical, monitoring system called the "Plant Process Computer" crashed. Both systems had redundant analog backups that were unaffected by the worm, but, "The unavailability of the SPDS and the PPC was burdensome on the operators," notes the March advisory.

It took four hours and fifty minutes to restore the SPDS, six hours and nine minutes to get the PPC working again.

FirstEnergy declined to elaborate on the incident. The company has become the focus of an investigation into last week's northeastern U.S. blackout. Though the full cause of the blackout has yet to be determined, investigators have reportedly found that it began when an Ohio high-voltage transmission line "tripped" after sagging into a tree. An alarm system that was part of FirstEnergy's Energy Management System failed to warn operators at the company's control center that the line had failed.

Asked if last week's "Blaster" worm might have had a hand in the alarm system failure, just as Slammer disabled the Davis-Besse safety display panel, FirstEnergy spokesman Todd Schneider said, "We're investigating everything right now."

"I have not heard of anything like that," added Schneider. "The alarm system was the only system that was not functioning."

SCADA Issues

The Davis-Besse incident was not Slammer's only point of impact on the electric industry. According to a document released by the North American Electric Reliability Council in June, Slammer downed one utility's critical SCADA network after moving from a corporate network, through a remote computer to a VPN connection to the control center LAN.

A SCADA (Supervisory Control and Data Acquisition) system consists of central host that monitors and controls smaller Remote Terminal Units (RTUs) sprinkled throughout a plant, or in the field at key points in an electrical distribution network. The RTUs, in turn, directly monitor and control various pieces of equipment.

In a second case reported in the same document, a power company's SCADA traffic was blocked because it relied on bandwidth leased from a telecommunications company that fell prey to the worm.

Reports on the effect of last week's Blaster worm on the electric grid, if any, have yet to emerge.

The Slammer attacks came after years of warnings about the vulnerability of power plants and electric distribution systems to cyber attack. A 1997 report by the Clinton White House's National Security Telecommunications Advisory Committee, which conducted a six-month investigation of power grid cybersecurity, described a national system controlled by Byzantine networks riddled with basic security holes, including widespread use of unsecured SCADA systems, and ample connections between control centers and utility company business networks.

"[T]he distinct trend within the industry is to link the systems to access control center data necessary for business purposes," reads the report. "One utility interviewed considered the business value of access to the data within the control center worth the risk of open connections between the control center and the corporate network."

Future Safety Concerns

An energy sector cybersecurity expert who's reviewed nuclear plant networks, speaking on condition of anonymity, said the trend of linking operations networks with

corporate LANs continues unabated within the nuclear energy industry, because of the economic benefits of giving engineers easy access to plant data. An increase in plant efficient of a couple percentage points "can translate to millions upon millions of dollars per year," says the expert.

He says Slammer's effect on Davis-Besse highlights the dangers of such interconnectivity.

Currently, U.S. nuclear plants generally have digital systems monitoring critical plant operations, but not controlling them, said the expert. But if an intruder could tamper with monitoring systems like Davis-Besse's SPDS, which operators are accustomed to trusting, that could increase the risk of an accident.

Moreover, the industry is moving in the direction of installing digital controls that would allow for remote operation of plant functions, perhaps within a few years, if the NRC approves it. "This is absolutely unacceptable without drastic changes to plant computer networks," says the expert. "If a non-intelligent worm can get in, imagine what an intruder can do."

Jim Davis, director of operations at the Nuclear Energy Institute, an industry association, says those concerns are overblown. "If you break all the connections and allow no data to pass from anywhere to anywhere, you've got great security -- but why'd you put the digital systems in the first place?," says Davis.

Davis says the industry learned from the Davis-Besse incident, but that the breach didn't prove that connections between plant and corporate networks can't be implemented securely. "You can put a well-protected read-only capability on a data stream that provides you reasonable assurance that nobody can come back down that line to the control system," says Davis.

Last year the NEI formed a task force to develop updated cybersecurity management guidelines for the industry. The results -- which will be secret -- are expected within a few months. As part of a research effort earlier this year, the NEI's task force worked with the NRC and a contractor to review cybersecurity at four nuclear power plants. The details of the review are classified as "Safeguards" material, but Davis says the investigation found no serious problems. "There are no issues that generate a public health and safety concern," says Davis.

"Sometime people get very anxious about digital systems and what you could or couldn't do with digital systems, but in lots of cases you've got switches and valves and little override buttons on this thing and that thing that could cause a component to shut down as quickly as any digital system," Davis says.

Despite the Slammer breach, FirstEnergy was apparently not in violation of NRC's limited, and aging, cybersecurity regulations. For its part, the commission wouldn't comment on the incident. The NRC has faced fierce criticism for not acting sooner to curb far more serious physical safety problems at the plant.

[Privacy Statement](#)

Copyright 2006, SecurityFocus