washingtonpost.com

Cyber Incident Blamed for Nuclear Power Plant Shutdown

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

The computer in question was used to monitor chemical and diagnostic data from one of the facility's primary control systems, and the software update was designed to synchronize data on both systems. According to a report filed with the Nuclear Regulatory Commission, when the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown.

Southern Company spokeswoman Carrie Phillips said the nuclear plant's emergency systems performed as designed, and that at no time did the malfunction endanger the security or safety of the nuclear facility.

Phillips explained that company technicians were aware that there was full two-way communication between certain computers on the plant's corporate and control networks. But she said the engineer who installed the update was not aware that that the software was designed to synchronize data between machines on both networks, or that a reboot in the business system computer would force a similar reset in the control system machine.

"We were investigating cyber vulnerabilities and discovered that the systems were communicating, we just had not implemented corrective action prior to the automatic [shutdown]," Phillips said. She said plant engineers have since physically removed all network connections between the affected servers.

Computer security experts say the Hatch plant incident is the latest reminder of problems that can occur when corporate computer systems at the nation's most critical networks are connected to sensitive control systems that were never designed with security in mind.

Specifically, experts worry that vulnerabilities were introduced into the systems that regulate the electrical grid as power companies transferred control of generation and distribution equipment from internal networks to supervisory control and data acquisition, or SCADA, systems that can be accessed through the Internet or by phone lines, according to consultants and government reports.

The move to SCADA systems boosts efficiency at utilities because it allows workers to operate equipment remotely. But experts say it also exposes these once-closed systems to cyber attacks.

"Part of the challenge is we have all of this infrastructure in the control systems that was put in place in the 1980s and '90s that was not designed with security in mind, and all of sudden these systems are being connected to [Internet-facing] business networks" said Brian Ahern,

president and chief executive of Industrial Defender Inc., a Foxborough, Mass.-based SCADA security company.

Joe Weiss, managing partner at Cupertino, Calif.-based Applied Control Solutions, said Hatch is not the only plant that has suffered this type of unusual event. But he said it is one of a handful of public events of this type because the Nuclear Regulatory Commission documents all unusual events, in contrast to non-nuclear facilities that do not make their unusual events public.

"Consequently, it is expected that non-nuclear facilities have experienced similar events," Weiss said. "The Hatch event illustrates the unintended consequences that could occur when business information technology systems interconnect with industrial control systems without adequate design considerations."

Weiss said unplanned, automatic shutdowns such as what happened at the Hatch plant are costly, forcing utilities to purchase power from other parts of the grid to the tune of about $1 million a day. But more importantly, Weiss said, automatic shutdowns unnecessarily challenge nuclear safety systems.

"Anytime you have to shut down, especially with an automatic shutdown, you're challenging the safety systems," he said. "What happened [at Hatch] was absolutely what the plant was designed to do, but there's always that chance that something could go wrong."

The NRC has for years had regulations in place that require that all plants be able to defend against cyber attacks. But the agency is still in the final stretch of implementing more specific cyber-security regulations that would require plants to detail their plans for defending their digital networks as a condition of maintaining their operating license, said Scott Morris, deputy director for reactor security at the NRC.

"The plants are expanding their use of digital technology to put more megawatts on the grid, and because of that these lessons are going to occur," Morris said. "But our expectation is that when these types of events happen, that [plant operators] correct the problem and share the information broadly with the rest of the industry."

Unplanned nuclear plant shutdowns used to be a fairly common event, but not anymore, Weiss said. In fact, he said, another shutdown of a U.S. nuclear plant was also precipitated by a cyber event. In August 2006, Unit 3 of the Browns Ferry nuclear plant went into a shutdown after two water recirculation pumps failed. An investigation found that the controllers for the pumps locked up due to a flood of computer data traffic on the plant's internal control system network.

Weiss said many people in charge of SCADA systems have sought to downplay the threat that hackers pose to these complex networks. But he cautioned that internal, accidental cyber incidents at control system networks can be just as deadly as a carefully planned attack from the outside.

In June 1999, a steel gas pipeline ruptured near Bellingham, Wash., killing two children and an 18-year-old, and injuring eight others. A subsequent investigation found that a computer failure just prior to the accident locked out the central control room operating the pipeline, preventing technicians from relieving pressure in the pipeline.

"To people in the IT world, cyber means 'attacks,' but what I tell people is that in our world the predominant cyber events are unintentional," he said. "The flip side of that is if it can happen unintentionally, it can probably be caused intentionally and be a whole lot worse."

News of the Hatch incident also comes as the cyber-security posture of the electric and nuclear power industry is coming under increasing scrutiny from Congress and government investigators. Last month, the Government Accountability Office issued a scathing report about

cyber security weaknesses at the Tennessee Valley Authority, the nation's largest public power company and operator of three nuclear plants, including Browns Ferry.

The GAO found that TVA's Internet-connected corporate network was linked with systems used to control power production, and that security weaknesses pervasive in the corporate side could be used by attackers to manipulate or destroy vital control systems. The agency also warned that computers on TVA's corporate network lacked security software updates and anti-virus protection, and that firewalls and intrusion detection systems on the network were easily bypassed and failed to record suspicious activity.

View all comments that have been posted about this article.

Post a Comment

View all comments that have been posted about this article.

You must be logged in to leave a comment. Login | Register

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the full rules governing commentaries and discussions. You are fully responsible for the content that you post.