



COMPUTERWORLD

Print Article Close Window

DHS quietly dispatching teams to test power plant cybersecurity

Agency moved to create teams to combat increasing attacks against power plants around the world, AP report says

Jaikumar Vijayan

August 4, 2010 ([Computerworld](#))

The Department of Homeland Security (DHS) is quietly creating specialized teams of experts to test industrial control systems at U.S power plants for cybersecurity weaknesses.

According to an Associate Press report today, DHS has so far created four teams to conduct such assessments, according to Sean McGurk, director of control system security. McGurk told the news service that 10 teams are expected to be in the field next year as the program's annual budget grows from \$10 million to \$15 million.

McGurk did not immediately respond to a *Computerworld* request for an interview. However a DHS spokeswoman this afternoon confirmed the DHS plan as detailed in the [Associated Press story](#).

She said the special teams are part of an Industrial Control Systems Computer Emergency Response Team (ICS CERT) that DHS has been building over the past year in response to worldwide cybersecurity threats against industry control systems.

The teams are being set up to help companies in critical infrastructure industries respond to and mitigate cyber incidents affecting industrial control systems, she said.

Each DHS team is said to be equipped with forensic tools, cables, converters and data storage equipment to be used to probe for and fix security vulnerabilities in control systems.

According to the report, the specialized DHS teams conducted 50 security assessments at power plants in the past year. In addition, teams were dispatched 13 times to investigate cyber incidents -- nine were found to be cyber intrusions and four were caused by operator error.

As an example, the AP story cites the infection of nearly 100 computers at a utility with the Mariposa botnet code. The infection was caused by the inadvertent attachment of an infected flash drive to a company laptop.



Concerns over such attacks have risen heightened sharply following the recent discovery of a malicious software program written specifically to exploit [vulnerabilities in Supervisory Control And Data Acquisition \(SCADA\) systems](#).

SCADA systems are used to control critical equipment at power companies, manufacturing facilities, water treatment plants and nuclear power operations. Many of the systems are relatively old and are thought to contain numerous vulnerabilities.

The malicious code, called [Stuxnet](#), is designed to exploit a Windows Zero Day flaw to find and steal industrial data from SCADA systems running Siemens Simatic WinCC or PCS 7 software. So far the malware is thought to have infected more than 15,000 computers worldwide, mostly in Iran, Indonesia and India.

Though the code is ostensibly designed to steal industry secrets, its ability to cause far worse harm raised considerable alarm among security experts.

Until fairly recently, most SCADA systems ran on segmented networks which made them relatively safe from external attacks. However, [many utility companies](#), including the largest ones, have more recently started to connect SCADA systems to broader businesses networks with direct Internet connections, making them easier to attack.

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at [@jaivijayan](#), or subscribe to [Jaikumar's RSS feed](#) . His e-mail address is jvijayan@computerworld.com.