

COMPUTERWORLD

Security

 Print Article

 Close Window

Hackers break into water system network

Robert McMillan

October 31, 2006 (IDG News Service) An infected laptop gave hackers access to computer systems at a Harrisburg, Pa., water treatment plant earlier this month.

The plant's systems were accessed in early October after an employee's laptop computer was compromised via the Internet, and then used as an entry point to install a computer virus and spyware on the plant's computer system, according to a report by ABC News.

The incident is under investigation by the Federal Bureau of Investigation, but no arrests have been made in the matter, said Special Agent Jerri Williams of the FBI's Philadelphia office. The attackers are believed to have been operating outside of the U.S.

Williams said that the hackers do not appear to have targeted the plant. "We did not believe that they were doing it to compromise the actual water system, but just to use the computer as a resource for distributing e-mails or whatever electronic information they had planned," she said.

Still, the FBI is concerned that even without targeting the system itself, this malicious software could have interfered with the plant's operations, Williams said.

Had the breach targeted the water plant, it could have had grave consequences, according to Mike Snyder,

security coordinator for the Pennsylvania section of the American Water Works Association. "It's a serious situation because they could possibly raise the level of chlorine being injected into the water... which would make the water dangerous to drink."

After the terrorist attacks of Sept. 11, 2001, computer security at U.S. water systems was beefed up, but water systems may still be tied to administrative networks that are connected to the Internet, Snyder said. "Sometimes if a hacker is pretty good, he can get into the computer via the administrative network," he said.

In the Harrisburg case, a laptop computer was apparently the source of the intrusion. Snyder said that laptops are used in the industry because water systems often have many different locations that need to be monitored. "Because of the way the water systems work, it is convenient to be able to use a laptop to check tank levels."

The U.S. Environmental Protection Agency knows of no other similar incidents occurring in the region, said Rick Rogers, the chief of the agency's drinking water branch for the mid-Atlantic region.

Rogers was not able to comment directly on the matter, since the breach is under investigation. "We are looking into it and working with the state and the water utility industry," he said. "But it is a concern that somebody was able to get into a system like this."