Print - Investigator: Cyber attack bigger threat than Sandy | wkyc.com

11:56 PM, Oct 31, 2012

CLEVELAND -- As electric companies continue to restore power from Hurricane Sandy, a potentially more devastating threat is looming -- from cyber criminals who may try to get control of the power grid.

Cyber criminals and nations are increasingly using the Internet, as well as traditional spying techniques, to infiltrate the computer networks of power companies and the larger electrical grid that distributes power between states.

Failing to address these cyber attacks could lead to "cyber Pearl Harbor," U.S. Defense Secretary Leon Panetta said last month.

Some experts have estimated that a successful widespread attack could take months -- months -- to fix.

"They're looking for system vulnerabilities, whether that's for the ability to affect power production (or) to take down the grid," said Todd A. Snitchler, chairman of the Public Utilities Commission of Ohio.

The National Security Agency says computer hackers are ramping up efforts to take down the U.S. power grid, with a 17-fold increase on attacks to the nation's critical infrastructure in the last two years.

"They're growing from disruptive to destructive and our country has the bulk of this network," Gen. Keith Alexander, the NSA chief, told the Aspen Security Forum in August. "We're the most vulnerable and we need to do something about it."

In the last two years, nine power companies reported cyber attacks they considered large enough to report to the federal government, according to the North American Electric Reliability Corporation.

The U.S. Department of Homeland Security, meanwhile, said that cyber incidents affecting control systems of companies in the electricity sector have increased from three in 2009 to 25 in 2011, the U.S. Government Accountability Office reported.

That includes three malware samples that Homeland Security uncovered at a bulk electric provider and a utility company last year.

"Just about every day there is somebody or something that is trying to get into our system," said FirstEnergy spokesman Mark Durbin, noting that the company so far has been able to thwart those attacks. "Our job, obviously, is to make sure that doesn't happen."

If hackers do get in, they can send power generators out of control or shut them down.

"The economic costs are huge and the restoration process is also very slow," said Case Western Reserve University Prof. Ken Loparo.

Loparo said the system is designed to prevent large-scale attacks that would take down the electrical grid that distributes power to local electric companies, which in turn, send it to homes and businesses. That doesn't mean it couldn't happen, however.

"Some of these (computer viruses or worms installed by cyber attackers) may be actually fairly easy to detect," Loparo said, "but some of them may require a complete rebuild of the system, essentially, you have to get rid of everything and start from scratch ... because you can't get the virus or malware out.

The threat is about get much bigger as the nation's 3,000 power utilities continue to build the so-called "Smart Grid."

Where the current system only sends power to your home or business, the Smart Grid will use "smart meters" that allow customers can talk back to the utility over the Internet.

Currently, about a third of Ohio's customers have these "smart meters."

The Smart Grid is supposed to help customers reduce energy consumption because they can see their usage in real time and reduce usage accordingly.

It's also supposed to prevent widespread outages by automatically rerouting around trouble spots.

But experts say the Smart Grid also gives cyber criminals new ways to infiltrate the system.

A few years ago, security company IOACTIVE performed a demonstration on how susceptible these smart meters can be. It hacked into one smart meter in Seattle and gained control of entire neighborhoods.

While a hacker couldn't get into the larger Smart Grid through these meters, it could hold individual customers hostage.

"We're behind the ball with security," said Trevor Niblock, director of energy services at IOActive. "They don't fully have a grasp on even what the threats and risks are in cyber space."

Just last month, hackers broke into a company that designs software for the Smart Grid, taking files that could give them insight into how to launch a bigger attack.

So who's behind these attacks?

Aunshul Rege, of Temple University, said it could be individual hackers looking for a thrill, groups angry with U.S. energy policies, or even organized crime groups looking to extort money. Such extortion plots have already happened in Brazil and India.

"If you want your grid to function, you better pay up," said Rege, who has studied these hackers.

But the real dangers are other nations like Iran, Russia, and China, Rege said. They have the money, people and know-how to get inside.

"It's no longer cyber war or physical war," she said. "It's more a blended sort of attack."

The state says foreign countries are repeatedly trying to crack Ohio's electric grid.

"It's the level of sophistication, it's the type of attack being made, it's the continuous repeated force," said Snitchler. "Whether there's been penetration to the deepest levels of the system ... companies maintain that information very strictly. It's not something in the interest of sharing."

"No one has said yes" when Snitchler directly asked the utilities if they've been successfully hacked, he said.

Loparo says it's impossible to make the grid 100 percent secure.

"It's a matter of putting the right level of vigilance on that system, so that ... you know somebody has hacked into the system," he said.

The Obama Administration has a number of groups working on solutions. But Republicans this August killed a bill that would create strict, voluntary security standards on utilities.

Critics argued that any cyber security standards would place financial strains on companies.

Republicans, however, are pushing for more information sharing by the Department of Homeland Security on cyber

threats. They say that's not happening quickly enough now.