updated 9:17 a.m. EDT, Thu September 27, 2007

Mouse click could plunge city into darkness, experts say

STORY HIGHLIGHTS

- Sources: Similar attack could hurt generators that produce nation's electricity
- Experts fear attacks could cause damage that would take months to fix
- Department of Homeland Security said staged attack took place in March
- DHS official: A lot of risk has been "taken off the table" since experiment

Next Article in U.S. »

READ VIDEO INTERACTIVE

From CNN's Jeanne Meserve

WASHINGTON (CNN) -- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

art.dhs1.jpg

Department of Homeland Security video shows a generator spewing smoke after a staged experiment.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.

CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab.

In a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

DHS acknowledged the experiment involved controlled hacking into a replica of a power plant's control system. Sources familiar with the test said researchers changed the operating cycle of the generator, sending it out of control.

Watch the generator shake and start to smoke »

The White House was briefed on the experiment, and DHS officials said they have since been working with the electric industry to devise a way to thwart such an attack.

"I can't say it [the vulnerability] has been eliminated. But I can say a lot of risk has been taken off the table," said Robert Jamison, acting undersecretary of DHS's National Protection and Programs Directorate.

Government sources said changes are being made to both computer software and physical hardware to protect power generating equipment. And the Nuclear Regulatory Commission said it is conducting inspections to ensure all nuclear plants have made the fix.

Industry experts also said the experiment shows large electric systems are vulnerable in ways not previously demonstrated.

Don't Miss

- Investigators: Homeland Security computers hacked

"What people had assumed in the past is the worst thing you can do is shut things down. And that's not necessarily the case. A lot of times the worst thing you can do, for example, is open a valve -- have bad things spew out of a valve," said Joe Weiss of Applied Control Solutions.

"The point is, it allows you to take control of these very large, very critical pieces of equipment and you can have them do what you want them to do," he said.

Adding to the vulnerability of control systems, many of them are manufactured and used overseas. Persons at manufacturing plants overseas have access to control system schematics and even software program passwords, industry experts say.

Weiss and others hypothesize that multiple, simultaneous cyber-attacks on key electric facilities could knock out power to a large geographic area for months, harming the nation's economy.

See how America's power grid works »

"For about $5 million and between three to five years of preparation, an organization, whether it be transnational terrorist groups or nation states, could mount a strategic attack against the United States," said O. Sami Saydjari of the nonprofit Professionals for Cyber Defense.

Economist Scott Borg, who produces security-related data for the federal government, projects that if a third of the country lost power for three months, the economic price tag would be $700 billion.

"It's equivalent to 40 to 50 large hurricanes striking all at once," Borg said. "It's greater economic damage than any modern economy ever suffered. ... It's greater then the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II."

Computer experts have long warned of the vulnerability of cyber attacks, and many say the government is not devoting enough money or attention to the matter.

"We need to get on it, and get on it quickly," said former CIA Director James Woolsey on Tuesday.

Woolsey, along with other prominent computer and security experts, signed a 2002 letter to President Bush urging a massive cyber-defense program.

"Fast and resolute mitigating action is needed to avoid a national disaster," the letter said.

But five years later, there is no such program. Federal spending on electronic security is projected to increase slightly in the coming fiscal year, but spending in the **Department of Homeland Security** is projected to decrease to less than $100 million, with only $12 million spent to secure power control systems.

The North American Electric Reliability Corporation has adopted cyber security standards for the electric utility industry, and the Federal Energy Regulatory Commission has regulations in the offing. Some outside experts say neither go far enough to protect the industry from cyber attack.

Groups representing the electric utility industry declined to comment for this report.

Despite all the warnings and worry, there has not been any publicly known successful cyber-attack against a power plant's control system. And electric utilities have paid more attention to electronic risks than many other industries, adopting voluntary cyber-standards.

"Of all our industries, there are only a couple -- perhaps banking and finance and telecommunications -- that have better cyber-security or better security in general then electric power," Borg said.

And DHS notes that it uncovered the vulnerability discovered in March, and is taking steps with industry to address it.

While acknowledging some vulnerability, DHS's Jamison said "several conditions have to be in place. ... You first have to gain access to that individual control system. [It] has to be a control system that is vulnerable to this type of attack."

"You have to have overcome or have not enacted basic security protocols that are inherent on many of those systems. And you have to have some basic understanding of what you're doing. How the control system works and what, how the equipment works in order to do damage. But it is, it is a concern we take seriously."

"It is a serious concern. But I want to point out that there is no threat, there is no indication that anybody is trying to take advantage of this individual vulnerability," Jamison said.

Borg notes that industry will have to remain forever vigilant at protecting control systems.

"It will always be an ongoing problem. It's something we will have to be dealing with [for] lots of years to come," he said. E-mail to a friend

All About U.S. Department of Homeland Security

EMAIL SAVE PRINT

▸ **From the Blogs:** Controversy, commentary, and debate

Top News

Senators 'troubled' after Rice meeting

Bergen: Senseless Benghazi obsession