

Hack raises fears of unsafe energy networks

By [Robert Lemos](#), CNET News.com

Published on [ZDNet News](#): June 13, 2001, 10:15 PM PT

-
- [Forward in](#)
- [EMAIL](#)
- [Format for](#)
- [PRINT](#)

A recent attack on the heart of California's power distribution center underscores the danger of connecting critical resources to networks that may never be truly secure from malicious hackers.

An intruder who cracked the security of two Web servers at the California Independent System Operator (ISO)--the nonprofit corporation that controls the distribution of 75 percent of the state's power--was inexperienced and benefited from human error and sheer luck, sources close to an investigation into the attack said this week.

The breach, which came to light following a *Los Angeles Times* report last Saturday, should remind those responsible for critical systems that simple mistakes can lead to disasters.

"We haven't learned to protect our critical infrastructure even though we have been working on this for a while," said Chris Rouland, director of internal research and development for network protection firm Internet Security Systems. "They did just about everything wrong in deploying systems in a hostile environment."

California's power grid has come under increasing scrutiny as soaring utility prices and rolling blackouts throughout the summer threaten to disrupt business in the state. On a national level, the threat to power networks is not an idle one.

In 1997, the National Security Agency--the United States' information watchdog--predicted such problems when a military exercise dubbed "Eligible Receiver" gained simulated control of the major power grids in Chicago, Los Angeles, New York and Washington in four days.

How it happened

The ISO hack took advantage of a security flaw in the agency's Solaris server systems, which was discovered in March. The attacker took control of two servers that were supposed to be protected by a firewall. In reality, the servers had not been secured and were connected directly to the Internet, according to sources close to the investigation.

Though the two Web servers were part of a development network, the attacker may have been able to work the initial breach into hacking more critical systems, said Rouland, who heads ISS's vulnerability assessment team, dubbed X-Force.

"Once the attacker gets a hold of a perimeter system, it gets them in the door and they can frequently leverage that into accessing the rest of the network," he said.

In addition to connecting the servers directly to the Internet, the Cal-ISO system administrators left the servers with all the software installed by the default setup, leaving numerous vulnerabilities open to exploitation.

The system also lacked the ability to collect a record of events in a secure place, instead leaving them on the computers that the intruder could access. The investigators could not easily detect which files had been changed. A rudimentary root kit--a tool set used by Internet attackers to take total control of a system--had been installed, but other details could not be discovered.

"There was an obvious attempt made to penetrate our systems," said Greg Fishman, spokesman for Cal-ISO, who would not give any more details. "They were able to achieve minimal penetration into a system that we use to demonstrate software. This was never a threat to our core operations."

Even so, some questioned the Cal-ISO's wisdom of connecting a development system to the Internet, even if protected by a firewall, as originally intended.

"Testing a system doesn't require that it be on the Internet," said Jay Dyson, senior consultant for online security firm OneSecure. "I don't know what they were thinking putting the test system live on the Internet."

The security holes left the system wide open to any hacker of minimal skill--and the intruder in question, Dyson said, was an amateur.

"There is no elegance to this intrusion," Dyson said. "This is just a case of throwing enough mud and hitting something. A skilled hacker would have been able to hide his tracks better."

Turning up the heat

The fact that even an amateur could get into the company's networks has officials in the state's capitol putting pressure on the Cal-ISO.

"I think it is a matter of intense concern that we have an ISO that allowed a breach of security through what appeared to be sheer incompetence," said state Sen. Tom McClintock, R-Thousand Oaks.

McClintock has issued a request under California's Open Records Act for all the documents concerning the break-in. The intrusion was discovered on May 11, but legislators weren't informed even a month after the breach occurred.

This fact had McClintock up in arms.

"I am in the process of preparing a formal request to investigate this matter," he said.
"Very soon we will know more."