Government simulates cyber attack for training

Tabassum Zakaria, Reuters

The lights went out. Hackers had infiltrated the chemical company's computer network. The firm's own experts ran around from computer to computer trying to fight back and regain control.

"We're flying blind," the chief executive of the fictitious ACME chemical company said.

The cyber attack exercise was part of a weeklong training program that the Department of Homeland Security offers to industries to help them learn how to deal with intrusions into their computer networks.

The exercise is carried out in Idaho Falls where the Department of Homeland Security (DHS) has programs focused on cybersecurity for industries, in partnership with the Idaho National Laboratory, which conducts nuclear research and also has expertise in the technology used by many industries.

The city with a population of about 55,000 is surrounded by potato farms, has an airport with one baggage carousel, and a dairy that still delivers milk to homes.

DHS is concerned about growing cyber threats to industries and conducts the training exercise about once a month. The sessions, aimed at raising awareness about how to deal with a real cyber attack, have been attended by representatives of the energy, oil and gas, and transportation sectors, among others.

What is usually a 12-hour exercise was compressed into two hours in a demonstration for reporters attending a two-day media event that ended Friday.

The scenario was one of industrial espionage. ACME had built a new chemical product and the Barney Advanced Domestic (BAD) Chemical Co was trying to steal its "secret sauce" and disrupt operations to put the competitor out of business.

The BAD hacker penetrated ACME's firewall through a typical "phishing" attack by sending an email to the CEO that said "click here" to go to a website.

When the CEO clicks on the link, malicious software opens a tunnel for the hacker to get into the computer system and find the CEO's password.

The man playing the hacker in real life works for the Idaho National Laboratory where his job has been to hack into its computer systems to discover vulnerabilities.

GAME OF STRATEGY

Each team racks up points and can use them to buy devices either to help protect the network or pierce it.

"This is a game of strategy in how to best implement your defenses in an industrial control environment," said Marty Edwards, director of the DHS Control Systems Security Program. "This isn't all about technology, it's about people."

Some of the most successful teams defending their firm against hackers are the ones that had leaders who delegated responsibilities and had clear policies about how the company would respond if a cyber attack happened, he said.

The ACME CEO, whose actions allowed the hackers into the network in the first place, said he clicked on the emailed link because "it looked like something I should click on, it said click here."

As a result of the breach the chemicals being mixed spilled out of white vats into a metal basin underneath.

Greg Schaffer, a senior official at the DHS National Protection and Programs Directorate, said as adversaries evolve their methods, cybersecurity must also evolve.

"They figure out ways to get around the defenses that you deploy, and because they are changing their methodologies, we need to evolve and change ours on a regular basis. And I don't see that that's going to end," he said.

Schaffer said cybersecurity issues have a lot of focus in the U.S. government and are likely to be less affected by cuts than other parts of the budget.

But, he said, it was important to make sure that areas of the government not focused on cybersecurity as their main mission keep it as a priority when determining cost cuts.

"As budgets becoming tighter, prioritizing taking action for cybersecurity within other parts of the government is something we have to be vigilant about advocating for," he said.

(Editing by Vicki Allen)