CSO
SECURITY AND RISK

From: www.csoonline.com

Defcon social engineering contest stirs concerns

Challenge that requires contests to target companies and obtain information is making some organizations uneasy

by Joan Goodchild, Senior Editor, CSO

July 21, 2010

A capture-the-flag-style competition slated to take place at Defcon later this month has raised eyebrows at a number of companies who are concerned they will be embarrassed or negatively impacted in some way. CSO first reported the CTF challenge earlier this month in Defcon contest to spotlight social engineering. The challenge asks contestants to collect information about a "target" company, which they are assigned to by contest coordinators at the web site social-engineer.org.

"In the excitement some have expressed concern that contestants might act improperly or that government, companies or individuals might be adversely impacted. We want to put these concerns to rest," officials with social-engineer.org said in a release, reacting to the fervor over the event.

Chris Hadnagy, one of the site's founders, said he decided to issue the statement after hearing that due to the fear generated, many contestants who work for larger corporations were threatened with termination if they participated in the CTF. He stressed that the purpose of the contest is to raise awareness of the threat of social engineering, and challenge contestants to come up with creative, legal ways of obtaining information from companies — not to embarrass anyone or do anything that would cause target companies to feel victimized.

"The contest is structured to be good, clean fun. Our goal is to show how much information companies may inadvertently divulge to individuals making regular, legal inquiries using normal channels of communication," the statement reads. "The type of information we will be asking for will be things like the number of restrooms in the building, and the sort of candy that sells out from the vending machines first."

Officials at social-engineer.org said they have been working with attorneys at the Electronic Frontier Foundation to ensure that the rules make clear to contestants that their game play must be lawful. Among the rules:

- Contestants may not ask for or obtain financial data, passwords, or personal identifying information such as social security numbers or bank account numbers;
- Contestants may not attempt to falsify or falsify employment records;
- The list of target organizations will not include any financial, government, educational, or health care organizations;
- Contestants must keep it clean, for example, use of any pornography is banned.

Contestants that do not follow the rules will be disqualified.

"We hope our CTF will raise awareness and provide information that shows companies what they need to educate their workers about malicious social engineering attacks," the statement said. "Malicious social engineers never hold contests, never do press releases and never warn the world they will be calling, and they also never have rules."