COMPUTERWORLD

FBI sought data on Defcon 'social engineering' contest

Said to be satisfied with restraints placed on contestants seeking to gain data from corporate workers using social engineering techniques

Robert McMillan

July 30, 2010 (IDG News Service)

A Defcon contest that invites contestants to trick employees at U.S. corporations into revealing not-so-sensitive data has rattled some nerves.

Contest organizers have been called by the FBI and has seen warnings issued by security groups and the Financial Services Information Sharing and Analysis Center, (FS-ISAC) an industry group that provides information on security threats affecting the banking industry.

"The stories that I'm getting are a lot of financial people were really concerned that we were going to be targeting personal information and stuff like that," said Chris Hadnagy, operations manager at Offensive Security, a security training firm and organizer of the Defcon contest. These concerns are unfounded, he says.

Over the next three days participants will try their best to unearth data from an undisclosed list of about 30 U.S. companies.

The contest will take place in a room in the Riviera hotel in Las Vegas furnished with a soundproof booth and a speaker, so an audience can hear the contestants call companies and try to weasel out what data they can get from unwitting employees.

This is social engineering: the art of tricking people into disclosing information and doing things that they shouldn't.

Conference organizers have to walk a fine line when running a contest that focuses on real-world targets. But after consulting with Electronic Frontier Foundation lawyers, they've come up with a set of contest rules and -- more important -- a do-not-do list.

Contestants can't ask for sensitive data or passwords. They can't make their victims feel like they're at risk. They can't pretend to be law enforcement or generally do anything that feels wrong. "If something seems unethical – don't do it. If you have questions, ask a judge," the rules state.

What participants can do is collect data on less sensitive subjects such as, "who does your dumpster removal; who takes care of your paper shredding," Hadnagy said.

The winner will be selected by judges, based not only on the quantity of data collected, but also the general excellence of the social engineering work, he said. First prize: an Apple iPad.

Security companies are often give the green light to use social engineering techniques against their clients as a way to test what might happen in a real-world incident and identify weaknesses. In these tests, security experts will often try to sneak into secure areas or trick employees into giving up passwords with phishing e-mails, things that are prohibited in this contest.

The Defcon contestant's primary tool will be the telephone. Contestants have been allowed to do Internet reconnaissance on their targets, and they will get 20 minutes in the phone booth to call the target companies and attempt their attack.

Hadnagy sees the contest as an experiment, of sorts, and plans to compile a report analyzing what happens. "We started it up to raise awareness for social engineering and give a venue to learn what makes a good social engineer," he said. "The easiest route into a company is still people."

Last month the FS-ISAC issued a warning about the contest, which Hadnagy posted to his blog. "Financial institutions should be aware of this upcoming contest, and should brief their personnel, especially call centers and legal departments regarding this event," the advisory states.

Around the same time, Hadnagy got a call from the FBI's Cyber Division. "They had questions on what our intent really was and what we were doing and what our goals were with the contest," he said. He forwarded the contest's rules to the FBI. "Once I passed that through to them… I think that stopped a lot of the government concern," he said.

Defcon's founder Jeff Moss said Thursday that he has fielded a few inquiries as well, including one from the FS-ISAC.

They needn't worry. Targets companies will come from the technology sector and other industries, but there won't be any financial, health care, educational or government organizations, Hadnagy said.

Robert McMillan covers computer security and general technology breaking news for The IDG News Service*. Follow Robert on Twitter at @bobmcmillan. Robert's e-mail address is robert_mcmillan@idg.com*