NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2010/090310-women-did-well-on-defcon.html

Only 5 (all women) of 135 pass Defcon social engineering test

Contest results will be published next week, organizers say

By Robert McMillan, IDG News Service
September 03, 2010 03:40 AM ET

Of the 135 Fortune 500 employees targeted by social engineering hackers in a recent contest only five of them refused to give up any corporate information whatsoever. And guess what? All five were women.

Women in IT: The long climb to the top

That's one of the interesting data points that contest organizers gathered, following their widely publicized event, held at the Defcon hacking conference last month. Organizers are in Washington this week, briefing the U.S. Federal Bureau of Investigation on what they learned, but they expect to release a report with more details sometime next week.

Contestants targeted 17 major corporations over the course of the two-day event, including Google, Wal-Mart, Symantec, Cisco, Microsoft, Pepsi, Ford and Coca-Cola. Sitting in a plexiglass booth, with an audience watching, they called up company employees, trying to get them to give up information.

The contestants were extremely successful, said Chris Hadnagy, one of the event's organizers. Just one company didn't divulge the secrets participants were told to dig up, and that happened only because nobody could get a live body on the phone. "If we had been hired by each one of these companies to do a security audit on the social engineering side, almost every one of the companies would have failed," Hadnagy said.

Contestants weren't allowed to ask for truly sensitive information such as passwords or social security numbers, but they tried to find out information that could be misused by attackers, such as what operating system, antivirus software, and browser their victims used. They also tried to talk marks into visiting unauthorized Web pages.

One interesting discovery: half of the companies contacted are still using Internet Explorer 6, a browser known to have serious security holes. Another discovery: if contestants tried to get employees to visit an outside Web site, set up for purposes of the contest, they always succeeded, eventually.

The results show that even the most secure companies can be undermined by employees who do or say things they shouldn't.

And the threats are real, according to Christopher Burgess, a senior security advisor at Cisco, one of the companies targeted by contestants. "In real life, pretext calls happen in many, many companies," he said. "It's a well refined art in information collection."

People have called Cisco, claiming that their systems are down and that they're on urgent deadlines, trying to get employees to give out information that they shouldn't, Burgess said. "We train our personnel to recognize that social engineering is a means by which people manipulate others to perform actions or divulge sensitive information."

Cisco has made a lot of its security training procedures publicly available, so that other companies can learn from its experiences over the years.

Although Cisco was one of the companies targeted in the social engineering contest, Hadnagy isn't giving out information about any specific companies.

Still, after going over the contest results with Hadnagy, Burgess said that the contest showed that the training process never really stops. "You can't train once and go away," he said. "You have to keep this training fresh."

Many of the contestants got their information by pretending to be insiders who were doing audits or consultants filling out surveys.

According to Burgess, employees should know to put a stop to this type of pretexting. "If I took away one thing from the discussion, it's that the best defense is to train all of your personnel to validate who they are talking to if they don't recognize the voice, before sharing any information about your company."

Burgess didn't want to talk about why all of the people who shut down contestants were women.

According to Hadnagy, though, different attacks work against different people. And maybe the types of social engineering techniques used by the Defcon contestants just weren't ideal.

Still the five women performed admirably, he said. "Within the first 15 seconds, they were like, 'This doesn't seem right to me,' and they ended the call," Hadnagy said. Unfortunately, their co-workers didn't do so well.

"Obviously there was some kind of security awareness with their training," he said. Another factor may have been the fact that all of the contestants were men. "I think inherently women are more cautious when guys are involved," he said.

Less than half of the 135 people called during the course of the contest were women, Hadnagy said.

Three of the five women who shut down contestants were managers, and female managers are often the least likely to fall for social engineering attacks, according to Jonathan Ham, a principal with the Lake Missoula Group, a security consultancy that does social engineering tests for financial services firms. "They're going to be the least trusting, the most suspicious," he said. "At the upper level of experience and training, I will avoid the women and call the men if I can," he 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*

The IDG News Service is a Network World affiliate.