www.esecurityplanet.com/features/article.php/3896386
Back to Article

Companies Fail DefCon Social Engineering Security Test
By Thor Olavsrud
August 2, 2010

No matter how much expertise and money you put into securing your network and data assets—firewalls, security appliances, encryption, etc.—the human element remains a vulnerability.

That message was expressed loud and clear through a contest held in conjunction with the DEF CON 18 Hacking Conference in Las Vegas this past weekend: Of the 140 phone calls made by contestants to real employees of real companies in an effort to collect information about those companies, only five employees declined to give contestants the information they were seeking.

Employees at every single company called gave away information about their company that they shouldn't have.

Organized by Social-Engineer.org at DEF CON's request, the Social-Engineer.org CTF (capture the flag) "How Strong Is Your Schmooze" contest was intended to raise awareness about social engineering and the danger even non-skilled social engineers can present to companies that aren't prepared, according to Chris Hadnagy.

"We define social engineering as understanding what makes a person think, tick, and react and then using those emotional responses to manipulate a person into taking an action that you want them to take," Hadnagy, a co-founder of Social-Engineer.org and operations manager at security training and tools firm Offensive Security, said.

He further explained that social engineering can be used for positive or negative purposes, but one major negative use is as part of a malicious attack on a company. Social engineering can gain information that can be used to penetrate a network, or to trick an employee into visiting a malicious URL or opening a malicious email or PDF.

Hadnagy explained that Social-Engineer.org was founded as a resource to help companies become more aware of the threat posed by social engineering techniques and defend themselves against those techniques.

Ask and ye shall receive

The contest held this past weekend Las Vegas was intended to further raise awareness. The participants were not social engineering experts for the most part.

"The majority of the people that joined the contest were not professional security auditors or social engineers," Hadnagy said. "They thought it would be fun."

Two weeks ago, each contestant was given the name of a real company. The contestants were allowed to spend the two weeks prior to the contest using "non-invasive" techniques to compile a dossier on the company they had been assigned. They were not allowed to e-mail, telephone, or contact the companies in any way, but could seek any information made

freely available by the company on the Web.

Using the dossiers they compiled, the contestants then created a profile of the company they had been assigned. They used those profiles to plan an "attack vector," a strategy for getting employees of the target company to reveal the "flags," or pieces of information that the contest asked participants to uncover.

Hadnagy explained that the rules of the contest specifically forbid contestants from attempting to gain passwords, IP addresses, or other sensitive data. Instead, the flags included information like who handles a firm's tape backups, the browser and browser version an employee uses, the software used to open PDFs, whether a company has a cafeteria and who operates it, etc.

"If you can get someone to give you that information, most likely you could get someone to give you a lot more," Hadnagy said.

He noted that Social-Engineer.org was contacted by the FBI while creating the contest and made some alterations to the contest's structure at the FBI's request.

During DEF CON, contestants each had an opportunity to appear before a live audience. They were given five minutes to explain their strategy and then had 25 minutes to call their target company in an attempt to capture as many flags as possible. The calls were made from a soundproof booth and the audience was able to listen in via speaker.

Hadnagy said that some of the largest companies in the world were called, though no financial services firms were on the call list as the organizers considered any information they might provide to be too sensitive.

"Every single company that had an available human failed," Hadnagy said. "Five people out of 140 calls shut us down. But then we would call that same company back, get a different employee, and then we would own that company."

He added, "We saw a very wide range of techniques, from people calling as a very technical person looking for information from a sales department to people playing really dumb, pretending they didn't know anything at all about computers."

One contestant, he noted, didn't really ask questions. Instead, he made statements like, "I bet you're using Internet Explorer 8," and the employee he was speaking with would then confirm or deny the statement.

"He racked up a lot more points than we thought he would using that kind of vector," Hadnagy said.

Killing them with kindness

Another contestant managed to get the employee he called to visit a particular URL, even after the employee had expressed reservations about doing so. When the employee asked why he should visit the URL, the contestant told him, "It will make me feel better." That convinced the employee to visit the Web site.

"He could have very easily had malicious files on that Web site," Hadnagy said, adding that

the network of that company could have been compromised if the contestant had been malicious. "That individual should have stuck to his guns."

As the contest illustrates, any company with employees is vulnerable, and the bigger the company, the more employees it has, the more vulnerable it becomes.

"If a company has 10,000 employees, that's 10,000 opportunities that a malicious social engineer has to hack into your company," Hadnagy said.

The only solution, he explained, is continual education. Employees have to be trained to think before revealing information.

"When you're on the phone and they're friendly and they sound nice and they start asking you for information, the first thing you should ask yourself is if this person deserves this information," he said.

Social-Engineer.org plans to develop a report based on the results of the contest. Hadnagy said the report would be available through Social-Engineer.org in about three weeks.

Thor Olavsrud is a freelance writer and a former senior editor of InternetNews.com. He has covered operating systems, standards, telecom and security, among other technologies.

Follow eSecurityPlanet on Twitter @eSecurityP.