AustinPost
Published on *Austin* (http://www.austinpost.org)

Social Engineering – A Major Threat To Companies

By *gerardsanchez*
Created *08/02/2010 - 00:44*

Social Engineering is a hacking technique that tricks employees into giving out delicate and very important information about the company they work for. It does not involve any technical means like breaking into the company's own computer system, but simply traps and deceives employees into providing sensitive data.

A report from CNET News [1] said that a contest conducted at the Defcon conference highlighted the issue, showing how participants were able to hack ten major U.S. companies through **social engineering**.

Christopher Hadnagy, the operations manager for Offensive Security (a training and penetration testing company), stated that if there was a security audit, every single company would have failed.

During the Defcon conference, the selected contestants were provided 25 minutes to make phone calls to major companies and get as much sensitive information as they can. These calls were broadcasted simultaneously over their sound system. The contestant who could obtain the most information won the event.

The questions that were asked from the targets seemed so harmless that the employees failed to recognize that the answer they provided were already vital information. It did not include questions about the company's upcoming technology [2] or anything about their financial activity. The contestants asked questions such as what browser the company's employees used, what company provides dumpster service, and whether their company has a cafeteria, all of which demonstrate how **social engineering** is done.

They revealed that during the first day of the **social engineering** contest, no company kept them from getting such important data. Though some companies did, they were still able to call right back and get a different employee that was more willing to comply.

The organizers of this event [3] declined to give comments and observations about any of the companies targeted for the contest. They refused to disclose which companies are better or worse than the others in terms of protecting their organization's sensitive information.

The lead trainer of Offensive Security, Mati Aharoni, said that the point of this contest is not to shame anyone. It was built to bring awareness to the problem, which is probably the easiest way to hack a corporation today. It is believed that **social engineering** is the latest [4] uncomplicated means of hacking. He added that they don't really want to see any company getting harmed or getting in trouble with **social engineering**.

Aharoni also mentioned that the human resources department is the weakest and softest spot of the whole organization. The most used vector by hackers today is the easiest route, and that is usually the human element. He added that people went as far as opening up their e-mail clients, Adobe Reader, versions of Microsoft Word, and clicking on 'Help/About' and giving the exact version numbers of their software. According to him, the exact version number would provide a much higher level of success for an attacker.

The event is a manifestation that major companies still lack precautionary measures for countering such threats to their security. **Social Engineering** is certainly critical and companies need to take necessary measures to protect the confidentiality of their data and the overall organization.

Links:
[1] http://news.cnet.com/8301-27080_3-20012290-245.html?tag=topTechContentWrap;editorPicks
[2] http://www.austinpost.org/category/article-category/tech-biz/tech
[3] http://www.austinpost.org/category/article-category/events
[4] http://www.austinpost.org/