FUSION AUTHORITY

Defcon Conference Challenge Shows the Dangers of Social Engineering

Aug 05, 2010

By Dana Tierney, Senior Editor, Fusion Authority

Perhaps this year's DefCon conference taught corporate America the sensitive nature of boring details like patch status and the fate of discarded corporate reports.

A handful of US companies targeted by DefCon's social engineering challenge learned this the hard way. A conference-sponsored contest selected thirty targets and assigned them to contestants.

Several contestants later had to drop out however, because of concerns raised by their employers about publicity given to the contest, said contest organizer Chris Hadnagy. The winners did not want to be photographed, and contest organizers did not release their last names. They did, however, say that the winning contestant broke a near-tie by submitting a much better dossier on his target than the second place contestant, although the final scores were very close.

Hadnagy, operations manager at Offensive Security, a security training firm, wanted to be sure that the press understood that the FBI was not, as reported, concerned about the contest.

FS-ISAC, an information-sharing group for security in the financial services industry, did issue a warning about the challenge, which the group posted on its website. This warning may have triggered an inquiry from the FBI about the challenge. After discussing it with organizers, the agency said it would not interfere with participants' first amendment rights, but advised the group to acquaint themselves with the Gramm-Leach-Bliley Act. Because of this suggestion the group consulted the Electronic Frontier Foundation for advice and as a result decided not to include banks as targets.

The press contingent at DefCon debated the ethics of disclosing the names of those companies and of the individual employees who agreed to talk to DefCon social engineers.

A consensus emerged to protect individual employees, but name the companies, among them Microsoft, WalMart. Cisco, Apple, BP, Shell, Google, Procter & Gamble, Pepsi, Coca-Cola, and Ford. Every single company wound up with an information disclosure, despite the warning provided by the advance announcement of the contest. Some individual employees did refuse to provide information themselves and referred callers elsewhere.

As Offensive Security trainer Mati Aharoni pointed out at a press conference, a hacker with malicious intent would not have accepted the limitations the rules put on contest participants, who could not ask for account information or make the person they spoke to feel threatened by, for example, alleging that a data breach had already occurred.

But the contestants did gather information that would have been useful in a large-scale organized attack. For instance, the information about trash pickup could help an attacker find information in company dumpsters, historically fertile ground for data breaches. So learning trash pickup dates earned the player an extra seven points.

Information about backups and who handles that, and when *they* make pickups was likewise worth up to twenty-five points. The employee's own schedule and break times, as well as how long the employee has worked for the target company, each scored five points, presumably for the information's potential value for reassuring other contacted employees.

Employee termination processes and new hire orientation information got twenty points each, and getting the target to go to a URL was worth 50 points.

The operating system the company uses, its service pack, which mail client and which version, which browser and version as well as the antivirus system used by the company could potentially allow attackers to zero in on specific vulnerabilities.

Organizers said they hoped the contest raised awareness of social engineering. "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," they said on their website. "To some extent, we feel that our goal has been advanced already by this discussion," they added. They plan to release a report on their findings soon.

Dana Tierney is the Senior Editor at House of Fusion, where she causes authors to cry over their once-thought perfect articles. They recover, and their articles are better for it. But still, the sound of grown men weeping...

Add a Comment

Name:
Website:
Email Address:
Comments:

Subscribe: (If you subscribe, any new posts to this thread will be sent to your email address.)

Add Comment Reset

Home
Subscribe
RSS
Categories
Editorial
Specials
Community
News
Tech and Tags
Views
Reviews
Techniques
Security
Best of ColdFusion Talk
Knowledge Base
Blog Watch
Columns
Tipical Charlie
Quarterly Update
Data: How do you make it work for you
Do More, Code Less
ColdFusion 8 Special Edition
Focus on the User Interface
Special Business Issue
Object Oriented ColdFusion
ColdFusion MX 7 Features You Need to Know

del.icio.us | digg | Spurl | Simpy | Newsvine | BlinkList | Furl | reddit | BlogMarks | Yahoo! My Web | Ma.gnolia | Technorati