Bloomberg Businessweek Thursday August 5, 2010

IDG

How to steal corporate secrets in 20 minutes: Ask

July 30, 2010, 8:59 PM EDT

IDG By Robert McMillan

A few companies in the Fortune 500 need to upgrade their Web browsers. And while they're at it, a little in-house training on social engineering wouldn't be a bad idea, either.

Social engineering hackers -- people who trick employees into doing and saying things that they shouldn't -- took their best shot at the Fortune 500 during a contest at Defcon Friday and showed how easy it is to get people to talk, if only you tell the right lie.

Contestants got IT staffers at major corporations, including Microsoft, Cisco Systems, Apple and Shell, to give up all sorts of information that could be used in a computer attack, including what browser and version number they were using (the first two companies called Friday were using IE6), what software they use to open pdf documents, their operating system and service pack number, their mail client, the antivirus software they use, and even the name of their local wireless network.

The first two contestants made it look easy.

Wayne, a security consultant from Australia who wouldn't give his last name, was first up Friday morning. His mission: Get data from a major U.S. company. (IDG News Service has chosen not to report which companies fell for which attacks because of possible security risks.)

Sitting behind a sound-proof booth before an audience, he connected with an IT call center and got an employee named Ledoi talking. Pretending to be a KPMG consultant doing an audit under deadline pressure, Wayne got Ledoi to spill details, big time.

Wayne ignored Ledoi's request for an employee number and launched immediately into a story about how his boss was on his back, and how he really needed to get this audit finished. He worked his Aussie charm on Ledoi, who'd only been with his new employer for a month. Within minutes, it seemed Ledoi was willing to give Wayne pretty much any information he wanted -- at one point Ledoi even visited a fake KMPG Web page that Wayne had set up.

He ended the call promising to buy Ledoi a beer.

"What beer do you like?"

"Right now I'm on a Blue Moon kick."

In an interview after the call, Wayne couldn't believe his luck. "I was thinking they're a pretty big company and I know they did a lot of in-house security audits."

Later, contest organizers said his effort was the best of the day. But everyone who was targeted gave up information. Chris Hadnagy, one of the founders of the contest, believes the victims would have given away sensitive information such as passwords had they been asked. "They would have given pictures of their family if they'd asked for it," he said.

Contest rules prohibited asking for any sensitive information, or targeting certain types of organizations such as government or financial institutions. Even so, the contest rattled nerves even before it had started. Last month, Hadnagy received a call from the FBI asking about the contest.

Wayne, who has done this type of social engineering for 15 years in his day job as a security consultant, said he did about 20 hours of reconnaissance ahead of the contest. He knew how to reach the IT call center and what names to drop when he got through.

He conceded that he'd lucked out by getting such a green employee. But new employees make the best sources. "If you pick someone who's a high-up person in the company, you'll get nothing," he said. "They've got a lot to lose."

Contestant number two, Shane MacDougall, decided to skip the call center and go right for the security staff at another well-known company. He took a more buttoned-down approach, claiming to be conducting a survey for CSO Magazine.

The first person he reached knew what he was doing, and firmly but politely shut MacDougall down after refusing to answer a few questions, saying, "These are specific questions that I don't feel comfortable answering."

Contestants were given only 25 minutes to work. So with the clock ticking, MacDougall lucked out on his next mark, Ryan -- a contract employee in the security engineering department who had been with the company for two months. After a few softball questions about job satisfaction and the quality of the cafeteria food, he went for the hard data.

Ryan delivered: operating system: Windows XP, service pack 3; antivirus: McAfee VirusScan 8.7; e-mail: Outlook 2003, service pack 3; browser: IE 6.

MacDougall then told him to visit a website to collect his US$25 survey coupon, and Ryan complied.

The contest runs at Defcon through Sunday. The winner gets an iPad.

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

Related Articles

- IBM: Vulnerabilities Fell in 2009, but Other Risks Abound - CSO ...
- Cisco may call home TelePresence 'UMI'
- Cisco launches Cius tablet for business
- RSA 2009: Automation, Integration Key to Fighting Cyber Crooks ...