

Social Engineering: The Forgotten Security Threat

by Mike Mitchell

You've installed a firewall, proxy server, and DMZ to reduce the risk of network attacks. Passwords, smartcards, and biometric identification are in place for user authentication and authorization. Card access systems are used to restrict entry to the datacenter and secure locations. Now you can rest easy knowing that all possible precautions have been taken to mitigate the threat of network intrusion, protect customer and employee information, and guard physical equipment. But have your cyber-security efforts really covered all possible threats?

In his book, *The Art of Deception*, the infamous social engineer, Kevin Mitnick, reports a 2001 Computer Security Institute survey showing 85% of responding companies had detected security breaches within the last 12 months. Sixty-four percent reported that they had suffered financial losses due to these intrusions.

The Weakest Link

If security policies and procedures are not carefully planned, prepared, publicized, and tested, then your security program is incomplete. Security awareness is every bit as important as technology. The weakest link in having effective security controls is employee behavior. Policies and training are needed to guide employees when they are confronted with unusual requests.

The Social Engineer Attacks

When strong security technology is implemented, a cracker might well move on to an easier target. A social engineer, on the other hand, doesn't rely on sophisticated technology to invade his target. His tools are knowledge, persuasion, and deception.

This con man can use a telephone, face-to-face interaction, dumpster diving, or even social networks like Facebook and LinkedIn to gather bits of information from one employee and use it to extract additional information from other employees. Eventually he can put all the pieces together to get employees to access systems, search databases, or peruse files to attain his objective.

Who is this Social Engineer?

The social engineer could be a vendor, consultant, contractor, or complete stranger intent on stealing intellectual or physical property or simply getting information for a future attack. Even a disgruntled employee may be tempted to try social engineering as a means to "get even" with the company for some perceived injustice.

Social Engineering: The Forgotten Security Threat

by Mike Mitchell

Knowledge, Persuasion, and Deception

Mr. Mitnick gives this mind-boggling account of an employee of a company hired to develop a data backup system for the wire transfer room of Security Pacific National Bank in Los Angeles. This person observed and wrote down the process used to wire money. One day he memorized the daily code used to transfer funds. After work, he used the lobby telephone to call the wire room, pretending to be one of the company's international brokers (he had already gotten the broker's information). As the con unfolded, he was asked for a code he didn't have. He made another interoffice call and persuaded an employee to give him the code. He called the wire room back with the additional code and "authorized" the clerk to transfer ten million, two hundred thousand dollars to a Swiss bank account. A few days later, he flew to Switzerland to pick up his cash!

Employee Awareness is Critical

A small informal survey I conducted of my friends and acquaintances revealed that not one of them knew if their company had a security policy dealing with social engineering. None had received threat awareness training or instructions on how to combat this type of cyber-crime. Raising employee awareness through training and testing is a critical step in securing your company's assets.

I would like to hear from you about how your company handles security awareness training and if there are policies in place minimize the risk of social engineering threats. In return, I will send you a helpful list of tips you can use to start a policy for your company. Send me an email at mike@telexcellence.com.