We know that “social engineering” is an important tool for criminal hackers. Social engineering refers to lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can then be used to break into systems. Social engineering is based on deception and on violation of social norms of fairness and honesty.

Vulnerability analysis is a useful approach to measuring the success of INFOSEC policies; it’s especially useful when there are known vulnerabilities introduced into a system and the percentage of identification of those known vulnerabilities is used as a measure of the quality of the penetration testing itself.

Penetration testing is one tool that can support vulnerability analysis. By itself, however, penetration testing -- simply looking for a way to penetrate a security perimeter -- is an inadequate measure of security. The important issue is not that a single breach was possible; that’s almost inevitable if the attacker has enough time and determination to accomplish the breach. A wider perspective insists on identifying as many vulnerabilities as possible so they can be removed. The widest perspective analyzes the corporate culture of the target to understand why the vulnerabilities were present at all, then moves to fix the underlying processes so that new vulnerabilities can be prevented.

One question arises when planning such penetration analysis is whether social engineering techniques should be used. My consistent answer is “No, not unless you are prepared to do an awful lot of work before trying it.”

Why not use social engineering?

The problem is that deceit can have profoundly disturbing effects on the deceived. If you hire someone to lie to your employees, don’t be surprised if you generate a lot of anger and maybe even a few resignations. If the victim of social engineering makes a mistake and compromises security in this kind of test, you might find your organization facing a lawsuit for emotional suffering. At the least you will find a drop in morale. If your penetration testers violate the law or induce someone to violate the law you may be in serious trouble.

What kind of preparation can help to avoid these consequences?

I was speaking with the head of the lifeguards at a pool many years ago and learned that the lifeguard team would arrange for occasional, unannounced drills in the pool. She explained that the pool management had approved a plan whereby a lifeguard or member of the swim team would simulate distress so that the lifeguard on duty could practice responding. This exercise was done with thorough preparation: everyone on the roster was aware of the possibility that there would be a simulation. The timing was unannounced, but the fact that there would be a simulation was understood by all.

One of the points the lifeguard told me is that during the planning phase, some members of the
group raised concerns about lowering the thoroughness of response to an emergency if a lifeguard thought it might be merely a test. The group agreed explicitly that all apparent emergencies would be treated as real.

I think that we can apply the same principles in our own work.

First, as always when testing security, the attackers (whether internal or external) must obtain written authorization from the appropriate levels of management before any such analysis is carried out. Above all, employees should never attempt to test their organization’s security without such written authorization. People have gone to jail for “testing security” without permission.

When preparing for a penetration test that involves social engineering, everyone in the organization should be thoroughly trained to understand the techniques of social engineering before beginning the tests. The entire organization can prepare for social-engineering simulations as a team; no one is subjected to attempted deception without knowing that the experience was part of a training and awareness exercise. Even if someone falls for a trick, the emotional effect is far less than if the same error occurred without preparation. In an organization-wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering can be reduced.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet’s first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.