Extreme Social Engineering

Combating the Insider Security Threat - A Security Awareness Exercise

by Jason Bevis (CISSP, ISSMP)

Overview

This paper has been developed to address the human factor of security and the apparent weaknesses within organizations due to employees' lack of security awareness. The purpose is to provide organizations a simple solution for increasing security awareness and combating other malicious insider security threats through a series of social engineering exercises.

The Problem

A unique way to increase security awareness and mitigate insider security threats is through social engineering tactics. This new approach helps organizations evaluate their security policies, increase internal awareness, and reduce future risks on new project initiatives.

An article entitled "Insiders Pose the Biggest Threat to Data Security" (published by Vontu, Inc., CSO Forum, October, 2006) speaks to the issue of internal security: "Whether data security policies are violated inadvertently or maliciously, the results expose the company to embarrassment, lost business, costly lawsuits, and regulatory fines. Industry analysts have identified company insiders as the leading threat to data security." This is probably not a surprise to anyone reading this paper.

As an information security professional with more than thirteen years experience in the industry, I have come across many instances where employees inadvertently breach security over and over again. Many of these employees are not even familiar with their organization's internal security policies or controls. Often, it is the organization's outside consultants who are involved in implementing new projects. These consultants are generally even less familiar with security polices and controls. In my experience many large consulting engagements pose as much of a security risk as the regular internal employees performing their day-to-day jobs. We all know that there are employees and consultants who write down passwords and carelessly leave them on their desks where anyone can see them, throw confidential data into the trash can, or just outright talk too much during their coffee breaks. Who knows—you may be one of them!

The Solution

How do we solve the problem? We put in more firewalls. We install anti-virus software. We patch our systems rigorously. We require special authentication mechanisms. Why go to all this trouble to solve a problem that is, in fact, a human behavior issue? Kevin McKeown, a top investigator and advisor who spent the past 20 years sleuthing for Fortune 500 companies and government organizations, points out the limitations of technology: "No matter how great the technology is, it is no better than man and his collective shortcomings". The simple fact is that education and monitoring are the best solutions for mitigating insider security threats. There is a relatively simple social engineering solution that managers can implement for all new projects.

Solutions to insider threat problems can be very costly. After studying several different security methods, understanding the tactics used by someone of average confidence (e.g., con artist), and diving head first into social engineering, one of the most cost effective and educational solutions is for organizations to perform a unique solution involving social engineering to combat insider security threats. It requires complete anonymity, and it requires full management support. It is a "cloak and dagger" game where the organization assigns an insider to a project. The goals are to identify threats, mitigate risk, and educate both internal staff and contractors. All this must be done without exposing how it was done until after the assessment. I will describe in detail what is required to perform this social engineering scenario.

The Plan and Techniques

The idea is to assign an individual—we'll call that person the "social engineer"—to a project to assess the security of the project, its internal controls, and its team members. This individual's mission is to fit in as a normal worker in a project-related job function (or someone who sits in the same relative area) while remaining completely anonymous so as not to arouse suspicion. More importantly, the social engineer engages in as much social engineering and reconnaissance as possible to identify the internal controls and security risks associated with the project and group. The social engineer performs his or her regular duties so as not to raise suspicion. At the end of a specified time frame, the social engineer provides an executive report to management explaining the level of access obtained, summarizing critical information, and describing any other risks or issues with internal security controls. A list of possible solutions to remediate the problem should be also be included in this report.

To initiate this internal assessment, there are several tasks that should be performed:

1. Identify the project to assess
2. Identify the social engineer
3. Present the social engineer as an appropriate project resource
4. Perform social engineering tactics
5. Report the results
6. Provide a security awareness seminar

A risk assessment could be used to determine the appropriate priorities for the project. While not a requirement, it is a good practice to create a risk assessment to help prioritize funding for security controls. Ideally, the project should be selected based on the level of risk associated with the information involved and the financial value of the data if it were to be lost, stolen, or compromised via denial of service (DOS), fraud, or any other method. The key is to identify a project that is in the late stages of development or close to the production migration phase. This will enable the social engineer to get a good understanding of the project quickly, establish rapport with staff, and view firsthand how passwords and confidential information are passed around among co-workers.

Now let's get down to the details. First, you need to find your social engineer. There are several organizations that offer this type of service for a fee. Otherwise, you can use an internal employee who is unknown to project team members, or you can hire a new employee whose sole responsibility is to act as an social engineer, rotating from project to project. However, it may be difficult to use an existing employee unless your organization is very large because the resource may be too well known or may require a good deal of training before performing the task at hand. If an outside firm is used, it should be independent from the consulting groups who are involved in the projects.

The next step is to introduce the social engineer to the project team. With management support, this task should be very easy. Begin by identifying the resource needs for a particular project or create a resource need. Once the need for a resource has been identified, then position the social engineer as the best fit for the job. Do a little resume falsification and develop a new resume with experience that matches the open position. Most external firms have templates for different job descriptions that they use for their social engineers. Make sure the resume appears realistic, and stay as close to the truth as possible with all background information. Don't change education, employment history, or any other data that the individual may inadvertently talk about. Change only the job experience information. After reworking the resume, share it with the team, along with a recommendation from upper management to staff the position immediately.

Once the social engineer is introduced and begins to work as a regular project team member, the social engineer can then implement the following information gathering techniques:

- Dumpster diving
- Do me a favor
- Desktop snooping
- Coffee break analysis
- Shoulder surfing
- Keyboard logging
- CD dropping

Dumpster diving is the practice of rummaging through the trash to find useful scraps of information that have been discarded. The social engineer should attempt to collect as much paper trash as possible without being noticed. It might be easiest to do this at the end of each day**.** Information of value includes: passwords, user names, confidential information, system information, or anything else that may violate your organization's security policy. Analyzing this information could take many long hours at night, so it may be best to have the social engineer work a later shift and at times show up a little late for work. For this task the person performing the dumpster diving does not necessarily need to be part of the project team.

Do me a favor is the practice of being overly helpful. By offering advice and assistance, the social engineer establishes an immediate rapport with other team members—something the social engineer can cash in on later with his/her victims. For example, if a user has a hard time logging in, the social engineer may offer to help. This is a good time for the social engineer to get the unsuspecting team member to reveal their user name and password. The team member most likely will not ascribe any ulterior motives to the social engineer. Not only has the password been compromised, but the victim now feels that they owe the social engineer a favor.

Desktop snooping is similar to the practice of dumpster diving and enables the social engineer to obtain sensitive data by rummaging through easily accessible areas—like someone's desk. Some employees leave sensitive information on their desks. This is an ideal situation for some after-hours reconnaissance, searching people's desks to find confidential data.

The ***coffee break analysis*** (or the *smoking break analysis,* depending on your preference), involves friendly encounters with employees or contractors during breaks or lunch. Most employees or contractors will let down their guard in a situation outside of the work environment. This is a good time to gather as much information as possible, and it will typically be apparent to the victim that the social engineer is only trying to learn more about the project. Good topics of discussion are stories about login problems with a particular system due to an incorrect password or user name. The social engineer can also mention that he/she needs to find the person in charge of granting access to a particular system. This way, the social engineer can obtain key personnel access and possibly access to general system accounts that everyone shares. This analysis can be done after hours at social gatherings too.

Shoulder surfing, which is essentially looking over someone's shoulder to obtain sensitive information such as their password, is another tactic. This may be difficult to do with some individuals. It is much easier to obtain information if the social engineer is equipped with a small camera. The goal is to gather as much information as possible–contact lists, user names, or other confidential information. This tactic may not be warranted in less secure environments better used on trains and airplanes.

Keyboard logging is most effective in organizations that allow users to install local software to their desktops. The social engineer installs a basic keyboard logger and coerces individuals into using his or her computer to access an account. One this tests the overall controls around installing software to the desktop. Two, this is a great way to test authentication mechanisms and internal security policies. It also enables the social engineer to possibly gain immediate access to critical systems.

CD/USB dropping is a wonderful tactic that can be used to obtain sensitive information or remote access to a user's computer. The social engineer drops off a CD (USB key) or multiple CDs with malicious software in a high traffic area such as the front desk or bathroom. The CD is labeled with a tantalizing title, like payroll information or layoff list. Once the CD is inserted into a victim computer, the malicious software will run using the auto run feature or it will run when the user clicks an executable file. The malicious software could potentially open a back door into the victim's computer without their knowledge, allowing the social engineer to execute attacks from this recently compromised host.

Conclusion

There are many more techniques than those I've described. These are just a sampling of the main methods that can be used to identify risks in the project. After performing these types of tasks for a specified period of time, the next step is to prepare a report and educate the staff. The report should be presented in a clear and easy-to-understand format, so that management can use the information in awareness sessions with the project staff.

To reduce risk and educate staff, the awareness session should be presented in a friendly environment where no one is reprimanded or singled out. All project staff—both internal employees and consultants—should be invited to the presentation. You may want to call it an executive security presentation and make it mandatory for all employees. It might be a good idea to tape it and make it available to those who cannot make it to the meeting.

The goal is to present the information that was gathered and point out the possible risks that are posed. Examples of best practices should be presented for all the major risks. For instance, if throwing away sensitive information is a problem, then identify where the shredders are on the floor and describe the type of information that should be shredded. If the organization doesn't have shredders, the social engineer should recommend that shredders be placed in a particular area, so that employees can discard information in the appropriate manner. This presentation also provides an opportunity for the organization to communicate internal security policies. Your consultants should not feel threatened by the findings; instead, they will understand the need to pay more attention to security when working on projects in the organization. And, internal staff will improve secure practices through greater awareness.

This approach to social engineering is one way for organizations to apply cost-effective security controls that will help combat insider security risks through education and raising awareness.

References

"Insiders Pose The Biggest Threat to Data Security" CSO Focus Vol.2 No.1 October
http://www.cio.com/sponsors/100105_vontu.pdf

Mckeown, Kevin with Stern, Dave. "Your Secrets are my business" Pg247. November 2000.