Global Information Assurance Certification Paper

Enhancing Defenses Against Social Engineering

Today's security professional faces a constant battle to keep abreast of the latest technological advances in order to remain one step ahead of hackers, crackers, and script kiddies. The constant barrage of security bulletins describing new vulnerabilities, hot fixes, and patches to repair vulnerabilities, and new security products require security professionals to dedicate large amounts of time ensuring that the technology employed to protect an organization's assets is up to current standards. Oftentimes, lost in the shuffle of competing demands for time, is attention to the ancient art of social engineering.

M.E. Kabay defines social engineering as 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."[i] Other adjectives like flimflam man, con man, grifter, and confidence man are dated, but accurate descriptive terms used over the years to describe the age old endeavor of gaining access, information, and influence that one is not entitled to through exploitation of others. Oftentimes, social engineers gather reconnaissance on their targets that will enhance the possibility of successfully obtaining the desired information. Once they have obtained the information, they use it to bypass security measures and compromise the targeted system.

Social engineering bypasses the most sophisticated security tools available by focusing on the weakest link of the security chain, the human link. Focusing on the human link ensures that no computer security system is immune to social engineering. "There is not a computer system on earth that doesn't rely on humans. This means this security weakness is universal, independent of software, platform, network, or equipment. All computer security systems require some human intervention to function."[ii]

This paper focuses on some of the underlying reasons people are vulnerable to social engineering exploits, and how security professionals can use this knowledge to best minimize these vulnerabilities.

In an article entitled People Hacking[iii], Harl discusses the following exploits, and discusses how various personality traits enhance the possibility of successful social engineering. When present, these traits increase the likelihood of compliance:

Diffusion of responsibility - If the target can be made to believe that they are not solely responsible for their actions, they are more likely to grant the social engineer's request. The social engineer creates situations with many factors that obfuscate and dilute personal responsibility for decision making. The social engineer may drop names of other employees involved in the decision making process, or claim another employee of higher status has authorized the action.

Chance for ingratiation - If the target believes compliance with the request enhances their chances of receiving benefit in return, the chances of success are greater. This includes gaining advantage over a competitor, getting in good with management, or giving

assistance to an unknown, yet sultry sounding female (although often it's a computer modulated male's voice) over the phone. There is a belief in the hacker community that technological people who have the keys to the shop often lack the skills to carry on adequate social relationships. Social engineers are not above using any form of influence when attempting to gain information.

Trust Relationships - Often times, the social engineer expends time developing a trust relationship with the intended victim, then exploits that trust. Following a series of small interactions with the target that were positive in nature and problem free, the social engineer moves in for the big strike. Chances are the request will be granted.

Moral duty - Encouraging the target to act out of a sense of moral duty or moral outrage enhances the chances for success. This exploit requires the social engineer to gather information on the target, and the organization. If the target believes that there is a wrong that compliance will mitigate, and can be made to believe that detection is unlikely, chances of success are increased.

Guilt - Most individuals attempt to avoid guilt feelings if possible. Social engineers are often masters of psychodrama, creating situations and scenarios designed to tug at heartstrings, manipulate empathy, and create sympathy. If granting the request will lead to avoidance of guilty feelings, the target is more likely to comply. Believing that not granting the requested information will lead to significant problems for the requestor is often enough to weigh the balance in favor of compliance with the request.

Identification - The more the target is able to identify with the social engineer, the more likely the request is to be granted. The social engineer will attempt to build a connection with the target based on intelligence gathered prior to, or during the contact. Glibness is another trait social engineers excel at, and use to enhance compliance.

Desire to be helpful - Social engineers rely on people's desire to be helpful to others. Exploits include asking someone to hold a door, or with help logging on to an account. Social engineers are also aware that many individuals have poor refusal skills, and rely on a lack of assertiveness to gather information.

Cooperation - The less conflict with the target the better. The social engineer usually presents as the voice of reason, logic, and patience. Pulling rank, barking orders, anger, and annoyance rarely works for gaining compliance. That is not to say that these ploys aren't resorted to as a last ditch attempt to break unyielding resistance.

Social engineering exploits often fall into one of the following categories:

Direct request - Perhaps the most simple method of social engineering, and also the least likely to succeed. Here, the social engineer simply asks for the information with no set up. A direct request is often challenged and usually refused. This technique is seldom used due to the low probability of success.

Contrived situation - The more factors the target must consider in addition to your basic request, the more likely the target is to be persuaded. These additional factors may allow the target to create reasons for compliance other than personal ones. The social engineer may claim to have forgotten a password due to being on vacation, or need access to an area after his manager has left for the day. A person struggling with a stack of computers, cables or manuals might ask someone to hold a secure door open. Crises may involve day care, medical care, or looming deadlines. The social engineer attempts to heighten the target's belief that compliance is necessary, helpful, and appropriate. The social engineer typically gathers intelligence on the target organization and/or individual to make the exploit appear more plausible. Although the social engineer often seasons his ploys with facts, it is important to remember that the exploit does not need to be fact-based; only plausibility is required.

Personal Persuasion - Many social engineers are adept at using personal persuasion to overcome initial resistance. The goal is not to force compliance, but to raise the likelihood of voluntary compliance. Here, the social engineer uses persuasion to make the target believe they are in control of the situation, and have the ability to help out. The fact that the benefits to helping out are imaginary or non-existent is insignificant. It is the target's belief that they are making a choice to grant the request after a reasoned decision making process that leads to compliance.

The amount of involvement the target has in the request determines the type of arguments the social engineer makes. Highly involved targets such as system administrators, computer security officers and technicians are influenced most by strong arguments. Weak arguments made to highly involved persons produce counter arguments, and lessen the likelihood of compliance.

Conversely, persons with low involvement and/or little interest in your request such as security guards, custodial workers, and receptionists are more likely to base their decision to grant the request based on information other than the pros and cons of arguments. Low involvement persons tend to make decisions based other information such as the urgency of the matter, the number of reasons given for needing the information, or the status of the person making the request.

So, how can middle-management system administrators and security professionals harden the people perimeter of the enterprise? In an article entitled 'Social Engineering - IT Security Threat of Informatics, Kajava and Siponen conclude that "most people in any computing environment are not sufficiently aware or knowledgeable of IT Security[iv]." They recommend an Information Technology Security Awareness Program that includes security information, security acceptance, and guidelines to end-users and management. They also include caveats on personal privacy and penetration testing.

Educating employees about the risks of social engineering is the first line of defense against attack, and may prove to be the most difficult to accomplish. Although all of us are vulnerable to exploitation by social engineers, most employees do not take well to being told they are gullible enough to fall for some of the oldest tricks in the book.

Additionally, social engineers have devised new tricks, based on psychological and social traits many of us share. These traits include: the desire to be helpful to others, the desire to avoid unpleasant events for ourselves and others, the desire to appear competent in our profession, the desire to trust others, the tendency to accept what others say as being truthful unless proven otherwise, the desire to advance our own cause and career, the desire to be attractive to those we admire or desire, the desire to believe that those we deal with are honorable, and the desire to be perceived as a team member. Social engineers have developed a repertoire of exploits and schemes to take advantage of every one of these positive human traits. It is important to note that social engineering involves the artful melding of many of the tactics outlined above, into a coherent and plausible exploit prior to launching it. Social engineers are unlikely to 'wing it', and will do so only after a planful exploit fails, or unplanned variables confound the exploit.

One way to increase security awareness is to create an internal web site, or utilize email for safety tips and informational stories on social engineering drawn from current events.[v] Most people are drawn to stories about other people's misfortunes. If you doubt this statement, simply open a newspaper or turn on the television. The media is full of these types of stories because these types of stories appeal to people on many levels. One rarely hears discussion in the workplace about the good deeds done in the world. Instead, employees discuss current disasters, tragedies, and mishaps. Using stories drawn from actual exploits allows the security professional to bypass employee resistance to acknowledging that they are vulnerable to these types of exploits. Like the parables and fables of the past, these current event vignettes deliver information with a purpose. In this case, the information bypasses, or decreases an individual's resistance to increasing security consciousness. They also deliver to the reader useful information helpful in avoiding falling victim to the same type of exploits. The use of current and factual events lends an air of authenticity to, and increases the impact of the lesson. The security professional need only subscribe to several of the many electronic security bulletins in order to gather more than enough real life exploits for presentation. Using real current events increases the likelihood that these security stories will be read, discussed and internalized by their intended audience.

Simply raising awareness of what happened to the unfortunate 'other guy' increases resistance to these exploits in a non-threatening way. These precautionary stories inoculate the audience against vulnerability to social engineering exploits. To enhance the effectiveness of this technique, content can be modified based on the 'involvement level' of the intended audience. Using the information presented above, security officers can predict which type of exploits will be attempted on different types of employees. Both high and low involvement audiences can be exposed to the probable methods that will be used by social engineers in an effort to exploit them.

Additionally, current information on a wide range of information security topics can be included in this venue. Topics might include: viruses and trojans, hoaxes, cryptography, passwords, biometric authentication and so on. The idea is to include rather than exclude, and to accustom users to including security concerns into their daily tasks. The

hope is that users will begin to feel they are part of a security team, instead of the victim of yet another security requirement.

Awareness needs to be coupled with a sense of individual responsibility for security. The organization needs to believe, and deliver the message that security is the responsibility of every employee. Every employee needs to be reminded that the security of the organization is only as strong as its weakest link. Employees in jobs not usually associated with information security such as mail room employees, PBX operators, and custodial services need to hear and believe that they are as important as highly technical users in preventing intrusion through social engineering. Management needs to believe this to be the case. Management also needs to provide basic security policies and procedures for dealing with a wide variety of situations. Additionally, management needs to ensure employees know that adherence to these policies is mandatory and expected.

A more aggressive posture to deal with vulnerability to social engineering involves penetration testing. Penetration testing looks at organizational security from an external point of view. Penetration testing asks two basic questions:

1. Does what we have in place now for security do what we argue it is supposed to do?
2. Does what we do not have in place now allow us to do what we are not supposed to do?[vi]

Penetration testing consists of employees or agents of the organization attempting to gain access to privileged information using the same tactics used by social engineers. "The IT security professional wanting to execute a penetration test should take the intruder's posture, including the most valuable tools of the intruder: time and patience. Moreover, they should view it as something of a challenge, because unless they approach this testing with the same tenacity as an intruder, the test will be somewhat diluted."[vii]
Since these tactics are used against employees of the organization, penetration testing can conflict with individual privacy rights and company policies. M.E. Kabay, writing in Network World Windows Networking Newsletter dated 12/18/00 offers the following warning to those considering the use of penetration testing of vulnerability to 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 very least you will find a drop in morale. And if your penetration testers violate the law or induce someone to violate the law you may be in serious trouble.

The security professional is urged to get written permission from management and a buyoff from the legal department prior to undertaking this form of testing.

A social engineer with enough time, patience and tenacity will eventually exploit some weakness in the security of an enterprise. Employee awareness and acceptance of security

policies and procedures are an important asset in the battle against attackers. The best defense against social engineering attacks combines raising the bar of awareness among all employees, coupled with a sense of personal responsibility to protect the enterprise. Security professionals can begin this process by making available to all personnel, a broad range of anecdotal information relating to security topics, including social engineering, virus alerts and hoax information. Remember to include details about the consequences of successful attacks in terms of loss of customer confidence, market share, assets, or negative publicity. Employees at all levels need to believe that they are an important part of an overall security strategy designed to protect the organization, its assets, and its employees from the negative consequences of social engineering.

---

[i] Kabay, M. E.. "Social engineering simulations." Network World Windows Networking Newsletter, 12/18/00. URL: http://www.nwfusion.com/newsletters/sec/2000/00292157.html?nf

[ii] Harl. "The Psychology of Social Engineering." Text of Harl's talk at Access ALL AREAS III, 05/07/97. URL: http://www.vampi.users1.50megs.com/social.html

[iii] Harl. "The Psychology of Social Engineering." Text of Harl's talk at Access All Areas III, 05/07/97. URL: http://www.vampi.users1.50megs.com/social.html

[iv] Kajava, J and Siponen, M.. "Social Engineering - IT Security Threat of Informatics." URL:http://www.ifi.uio.no/iris20/proceedings/9.htm,

[v] Fennelly, Carol. "The human side of computer security." URL: http://www.unixinsider.com/swol-07-1999/swol-07-security.html

[vi] Kajava, J and Siponen, M.. "Social Engineering - IT Security Threat of Informatics." URL:http://www.ifi.uio.no/iris20/proceedings/9.htm,

[vii] Ceraolo. "Penetration Testing Through Social Engineering." Information Systems Security, Vol $. No. 4, Winter 1996.