Running Head: SOCIAL ENGINEERING DEFENSE FOR SMALL BUSINESSES

Social Engineering Defense for Small Businesses

Russell Morgan

East Carolina University

Abstract

Social Engineering is one of the more effective methods of compromising a company's information security. It is also one of the hardest methods to defend against. Electronic attacks can often be thwarted with technology, but social engineering attacks use human nature to bypass electronic security measures. Because social engineering exploits human nature it is one of the most dangerous threats that companies face.

Social Engineering Overview

In order to defend against social engineering attacks it is necessary to understand what social engineering is and why it is so successful. There are many definitions for social engineering. Among them are: "Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures" (Searchsecurity.com) and "Social engineering is the practice of obtaining confidential information by manipulation of legitimate users." (Wikipedia) One of the primary methods of manipulation is to ask the victim for help with a task. This is not a new tactic, nor is it confined to the information technology sector.

Social engineering is an evolution of what was previously known as a con game. (Dubin 2002) Confidence men, also known as con men or grifters, have been around for years. These people are masters at manipulating others, usually for financial gain. There are endless stories about con men and many have been portrayed in movies. One of the most well known con men was the subject of a major Hollywood movie starring Leonardo DiCaprio as Frank Abagnale. Abagnale began his career as a con man committing bank fraud during the 1960s. He moved from bank fraud to impersonation. Over time, he was successfully able to impersonate airline pilots, doctors and lawyers. He was eventually caught and served a prison sentence. After his release, he worked for the government for a short time, then he opened a consulting firm that helps businesses fight financial fraud. The fact that Abagnale could con his way into such professions as

airline pilot and doctor shows not only how good he was at the con game it also showed how effective a skilled con artist can be. (Wikipedia)

As technology evolved in the 1960s, 1970s and 1980s con men did as well. Con men came to be known as social engineers and one of their first major targets was the phone systems of corporations. Using what is known as phone phreaking social engineers were able to get free long distance calls that were charged to unknowing companies. Other successful scams involved letters that arrived via fax saying they were from a foreigner that needed financial help. These scams were elaborate and usually involved the foreign entity claiming to be in possession of or able to access a large amount of money. He would give the victim part of the money in exchange for help moving it out of the the country. All he needed was some seed money and a bank account number. These scams were so rampant they came to be known as the Nigeria 4-1-9 scam after the section of Nigerian law they violated. (Wikipedia)

As computer networks became common in the 1980s and 1990s, social engineers turned their attention away from phone and fax systems and towards these new powerful networks. The downside to early networks for social engineers was that they often had to get into the company physically to access them. This increased the chance of being caught. With the explosive growth of the Internet in the 1990s a whole new avenue of attack was made available to the social engineering community. Most companies quickly joined the Internet revolution thus connecting them to potential customers as well as potential hackers. This allowed attacks against many more businesses and made it much easier to avoid being caught. One of the most famous or infamous hackers was actually more of a social engineer than a technical hacker. Kevin Mitnick used social engineering

methods to infiltrate several large companies such as Motorola and Sun Microsystems. He was eventually caught and served time in prison for his actions. Mitnick is now a reformed hacker and is running a security company and writing books offering help to protect against social engineering attacks. (Wikipedia)

Kevin Mitnick attributes the success of social engineering attacks to the fact that people are generally trusting. (Mitnick, Simon 2002) Because of this it is easy to see why people are the biggest weakness in an organization's security not their technological systems. (Granger 2006) If presented with the proper question or situation a low level help desk employee or security guard can compromise the best technical security on the planet.

Social Engineering Threats to Small Businesses

There are many different methods a social engineer can employ to gain access to your company's data. These are commonly divided into two categories; human based attacks and computer based attacks. Human based attacks rely on personal relationships while computer based attacks rely on technology to trick an individual into supplying the information. (Allen 2001) Among the various human based attacks are impersonation of various individuals either offering or needing help, dumpster diving and reverse social engineering. Most technological attacks today come from the Internet, but other methods exist as well.

A receptionist can be a very weak link in a company's security even if he or she has little technological access to company information. This is because they are the prime target for an attacker calling into the company. Sometimes a simple question to the receptionist will result in the exact piece of information the attacker needs, such as a

username and password. This is especially effective if the attacker pretends to be someone in a technical support capacity. (Allen 2001) Receptionist and switch board operators in the past were subject to phone phreaking attacks that involved the caller asking to be transferred to a certain extension thus giving them access to make long distance calls on the company's account. This vulnerability has been patched in most phone systems, but it is still a good example of how easy it is to manipulate users into compromising the company.

Another version of this attack can be much more complex and dangerous. In this form of attack the caller will ask the receptionist for what is seemingly harmless information. The information might include the names of managers, phone numbers or email addresses. This attack might require several phone calls with each phone call building upon the information gained in the previous phone calls. After gathering enough information the social engineer will be able to initiate his attack.

Dumpster diving is a threat for every company and may be more of a threat to small companies than large ones. The logic here is that large companies have policies and procedures in place for paper and equipment disposal. Many small companies do not have this and use standard trash service. The difference between what is considered sensitive information by the average employee and a social engineer can be huge. Things that seem harmless like company phone books, organizational charts, calendars and company letterhead can be used by social engineers to build their database of information. (Granger 2001) Once they have enough information they can employ an impersonation attack on the company or one of their business partners. Electronic media is another good source of information for social engineers. Many businesses simply

throw away old floppy disks and CD-ROMs. These can contain tons of information that would be of great value to an attacker. Improper disposal of old computers is another good source of information that many companies often overlook when thinking of data security.

Reverse social engineering is when the attacker causes a problem on the target's network or computer and then makes themselves available to fix the problem. When the problem is solved the attacker is viewed as the hero and has gained the trust of the target. This can be a much harder attack to pull off because it requires access to the network ahead of time. (Gragg 2002)

One form of computer-based attack can be perpetrated by giving away free software. This could be in the form of a floppy disk, CD-ROM or a flash drive that is sent to the company via postal mail. The media will claim to be a free tool or utility when in reality it contains a Trojan or some of other kind of malicious program. One recent example of this, with a slight twist, was when a security firm placed USB flash drives at random locations outside of a target facility. The drives contained a Trojan that would allow the security company to see which drives had been used. Out of 20 drives placed by the security firm 15 were used and plugged into company computers. (Stasiukonis 2006) These drives did not claim to be free software or anything else, but human curiosity still got them plugged into a computer behind the company firewall.

The primary threat that small businesses will face today is from the Internet. While there is a technical side to Internet based social engineering attacks they mostly rely on human nature. Some of the first attacks focused on email and would often have an attachment that was supposed to be a picture of Anna Kournikova or some other

celebrity. The attachment was actually a viral worm that once opened would spread itself to other users via the address book. (Allen, 2001) The previously mentioned Nigeria 4-1-9 scam has moved from postal mail and faxes to email. Since it is much easier and cheaper to send email this has become a very lucrative scam for the Nigerian perpetrators. (McLaughlin)

Pop-up windows are a popular attack vector for getting malicious software on computers. Some pop-ups target technical vulnerabilities, but many rely on social engineering techniques. Malicious pop-ups often come from sites that shouldn't be accessed at work, but sometimes they come from legitimate sites as well. They often claim to offer free anti-Spyware programs or other such services that sound good and helpful. Many times these are actually Trojan programs that will install back doors or other malicious software on your PC.

As a general rule humans are attracted to anything that is free. This is especially true on the Internet. There are many sites that offer free prizes if you fill out a form… Bundling malicious applications in with free software downloads is another possible attack avenue for social engineers. They will bundle their software in with a free video player or toolbar that you want or need. Along with the video player or toolbar you may also end up with Spyware or Ad-ware that you would otherwise never have installed. The RealPlayer media player was a good example of this. While the additional programs downloaded with it may or may not have been malicious they were certainly unwanted by most users.

Arguably the most effective online social engineering attack is known as Phishing. Phishing is the process of sending fraudulent emails directing the recipient to a

fake web site. Then they are asked to enter personal information. Some of these scams are very well done and effective, while others are very poorly done. Many Phishing emails focus on prominent online companies such as PayPal and Amazon.com. Other versions focus on banking institutions such as Bank of America or the Citi Group. Newer generations of Phishing emails are narrow in focus attacking specific small banks, for example.

Defense Strategies for Small Businesses

Small businesses are subject to the same threats as other businesses when it comes to social engineering attacks. One advantage small businesses have over large corporations however, is their size. While this is usually a weakness from a technology standpoint it can be viewed as a strength when dealing with social engineering attacks. In a large corporation with hundreds or thousands of employees there is little chance that you will know everyone in the company (Dolan 2004). Sometimes you may not even know all the people in your department if is it geographically separated. This is a big weakness in defending against social engineering attacks. In most small businesses it is not uncommon for an employee to know or at least know of all other employees.

The first step in securing any business from a social engineering attack is to develop a good security policy. Policies remove from employees the responsibility to make judgment calls about releasing information. If policies prevent giving out certain information, the employee can deny the hacker without fear of being unhelpful to a legitimate employee. (Granger 2002) Policies also need to be reviewed and revised from time to time. (Arthurs 2001) This can be tough in the small business environment where

most people wear many different hats, but a small amount of time creating and revising policies would seem insignificant in the event of a data compromise.

The best information security policy in the world is useless if it is not enforced. This means that management has to accept and support the policy. It also means that employees have to be trained about what the policy covers. If employees are never informed about the rules they cannot be held responsible for breaking them. (Dolan 2004)

Some of the items covered in the security policy are physical security, trash disposal, Internet usage rules and what kind of information can be given over the phone or through email. One very important item to include is a password policy. Employees need to be trained that their password is valuable and should not be given out to anyone.

Physical security seems like an easy topic, but sometimes the easiest things get overlooked and exploited. Some things that need to be in the policy have to do with locking computer rooms, locking the building itself and escorting non-employees at all times. Escorting all non-employees when they are in the office is important because it would not be all that hard for someone to impersonate a phone company repairman and gain access to your wiring closet or server room. If this impersonator is monitored while in the server room there is a much smaller chance of that they will cause damage. Someone walking around unescorted in your facility could also pick up lots of information simply by looking at papers on various desks.

The U.S. Government has a very detailed information classification system. While most small businesses do not need anything quite that elaborate there is still a lot of information that does not need to be released to the public or to a social engineer. Knowing what to shred and not to shred is important. In this part of the policy you would

decide on what information to put on your web site or to give out over the phone. As we have seen, an enterprising individual with knowledge of your company's reporting structure, some titles and a couple names can do a lot of damage.

Nearly all businesses have some kind of computer system these days. Computers have a very short lifespan and this means they will be replaced fairly often. Proper disposal of older hardware is critical since these devices can be a treasure trove of information about the company. When computers stop functioning or are replaced for performance reasons, steps need to be taken to make sure the hard drives are not useable by a malicious third party. Some people claim the only way to truly erase a hard drive is to physically destroy it. Others claim that just erasing the data is enough while others say using drive wipe utilities is the best method. This decision is ultimately up to the company, but the decision needs to be made and at a minimum the drives needs to be formatted before they are thrown away. Computer media is another big item to worry about here. Whether the media is printouts, floppy disks or CDs the same amount of thought needs to be put into the disposal of these items as was put into the hard drive disposal. Paper should be shredded and electronic media destroyed before it is put in the trash can or recycled. If all paper is not shredded, placing the dumpsters in a locked storage area is advisable to prevent dumpster diving. Remember that just because there is no financial or project data on paper that is thrown away the paper might still be useful to someone.

Threats from the Internet are probably going to be the main source of attack for most small businesses. The Internet is such a major tool now that it would be hard for most companies to operate without access to it. A good anti-virus program will detect

some Trojans, but no program will ever get them all. A recent posting on Microsoft's Anti-malware Engineering Team blog talking about a virus that was spreading through social engineering stated "Threats like this reinforce the idea that malware that exploits user weakness can be as dangerous as those threats which exploit software vulnerabilities and reinforces the value of up-to-date antivirus products as well as general user vigilance". (Lemos 2006) As mentioned in the Microsoft blog post user vigilance or awareness combined with training is the only defense against social engineering attacks. Users need to be trained to pay attention to pop-up windows and not just click yes to everything that comes along. Some of the newer pop-up scams are very good and hard to identify as malicious. Many claim to be and look like Windows errors in an attempt to get the user to click yes or OK on them. Training users to not forward chain emails is another good idea. Many of these email messages are infected with Trojans or other kinds of viruses that could be used to set up back door access to the network.

Phishing is probably the attack that small business users will encounter most often. Individuals were the first targets of Phishing attacks, but businesses are now becoming a target. (Benkoil 2005) Businesses typically have more money and with many of them using online banking now they are a prime target. Some of the newer Phishing scams are so well done it is even hard for experienced IT personnel to detect them at first glance. There is no way an average user will detect one. To combat this it is a good idea to train employees that no one will ever ask for financial information via email. Not opening the email and going to the fraudulent site is the only sure way to avoid compromise. Another good idea is to pay attention to the scam and the address it was sent to. For example I recently received a very well done Phishing email supposedly

from PayPal. It was a receipt for a purchase I had supposedly made and said that if I didn't make the purchase my account had most likely been compromised. They then offered a link for me to log in to and verify my account info. I may have had to dig a little deeper to crack this scam, but I thought about my PayPal account and realized that the email address the scam was sent to was not the email I had registered with PayPal. So a little thinking stopped that scam cold.

Conclusion

Creating and maintaining a sound network infrastructure is only half the battle when it comes to computer security. A good social engineer can gain access to your network without ever using a hacking tool simply by exploiting users that have legitimate access. Developing policies and training employees will greatly minimize the threat of social engineering. However, as noted by Kevin Mitnick in his book the *Art of Deception:* "As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element." (Mitnick, Simon 2002) This means that only through continuous training and vigilance can you ever hope to secure your network from the motivated social engineer.

*Arthurs, Wendy (2001) *A Proactive Defence to Social Engineering* Retrieved July 1, 2006 from http://www.sans.org/reading_room/whitepapers/engineering/

*Dubin, Lawrence (2002) T*he Enemy Within: A System Administrator's Look at Network security* Retrieved July 1, 2006 from http://www.sans.org/reading_room/whitepapers/engineering/

*Granger, Sarah (2001) *Social Engineering Fundamentals, Part I: Hackers Tactics* Retrieved July 10, 2006 from http://www.securityfocus.com/print/infocus/1527

*Granger, Sarah (2002) *Social Engineering Fundamentals, Part II: Combat Strategies* Retrieved July 10, 2006 from http://www.securityfocus.com/print/infocus/1533

*Granger, Sarah (2006) *Social Engineering Reloaded* Retrieved July 10, 2006 from http://www.securityfocus.com/print/infocus/1860

*Allen, Malcolm (2001) *The Use of 'Social Engineering' as a means of Violating Computer Systems* Retrieved July 1, 2006 from http://www.sans.org/reading_room/whitepapers/engineering/

*Gragg, David (2002) *A multi-Level Defense Against Social Engineering* Retrieved from http://www.sans.org/reading_room/whitepapers/engineering/

*Dolan, Aaron (2004) *Social Engineering* Retrieved July 1, 2006 from http://www.sans.org/reading_room/whitepapers/engineering/

Mitnick, Kevin D. and Simon, William L. (2002) *The Art of Deception*

McLaughlin, Abraham (2005) *Nigeria cracks down on email scams*, The Christian Science Monitor December 15, 2005 Retrieved July 10, 2006 from http://www.csmonitor.com/2005/1215/p07s02-woaf.html

Benkoil, Dorian (2005) *Phishing for business* Retrieved July 14, 2006 from http://reviews.cnet.com/4531-10921_7-6353531.html

Lemos, Robert (2006) *Social engineering trumps flaws?* Retrieved July 10, 2006 from http://www.securityfocus.com/print/brief/178

Stasiukonis, Steve (2006) *Social Engineering, the USB Way* Retrieved July 14, 2006 from http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

Anonymous (n.d.) *Social Engineering (security)* Retreived July 10, 2006 from http://en.wikipedia.org/wiki/Social_Engineering

Anonymous (n.d.) *Kevin Mitnick* Retreived July 10, 2006 from http://en.wikipedia.org/wiki/Kevin_Mitnick

Anonymous (n.d.) *Frank Abagnale* Retreived July 10, 2006 from http://en.wikipedia.org/wiki/Frank_Abagnale

Anonymous (n.d.) *Advance fee fraud* Retreived July 14, 2006 from http://en.wikipedia.org/wiki/Advance_fee_fraud#419_Fraud

Anonymous (n.d.) *Social Engineering (definition)* Retreived July 14, 2006 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html