Endpoint Protection - Symantec Enterprise

18-22 minutes

A True Story

One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm’s entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees’ names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering. (This story was recounted by Kapil Raina, currently a security expert at Verisign and co-author of mCommerce Security: A Beginner's Guide, based on an actual workplace experience with a previous employer.)

Definitions

Most articles I’ve read on the topic of social engineering begin with some sort of definition like “the art and science of getting people to comply to your wishes” (Bernz 2), “an outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system” (Palumbo), or “getting needed information (for example, a password) from a person rather than breaking into a system” (Berg). In reality, social engineering can be any and all of these things, depending upon where you sit.

The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this fact. No matter how many articles are published about network holes, patches, and firewalls, we can only reduce the threat so much... and then it's up to Maggie in accounting or her friend, Will, dialing in from a remote site, to keep the corporate network secured.

Target and Attack

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals. The Internet boom had its share of industrial engineering attacks in start-ups as well, but attacks generally focus on larger entities.

Finding good, real-life examples of social engineering attacks is difficult. Target organizations either do not want to admit that they have been victimized (after all, to admit a fundamental security breach is not only embarrassing, it may damaging to the organization's reputation) and/or the attack was not well documented so that nobody is really sure whether there was a social engineering attack or not.

As for why organizations are targeted through social engineering – well, it's often an easier way to gain illicit access than are many forms of technical hacking. Even for technical people, it's often much simpler to just pick up the phone and ask someone for his password. And most often, that's just what a hacker will do.

Social engineering attacks take place on two levels: the physical and the psychological. First, we'll focus on the physical setting for these attacks: the workplace, the phone, your trash, and even on-line. In the workplace, the hacker can simply walk in the door, like in the movies, and pretend to be a maintenance worker or consultant who has access to the organization. Then the intruder struts through the office until he or she finds a few passwords lying around and emerges from the building with ample information to exploit the network from home later that night. Another technique to gain authentication information is to just stand there and watch an oblivious employee type in his password.

Social Engineering by Phone

The most prevalent type of social engineering attack is conducted by phone. A hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user. Help desks are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator, so caller-ID is not always the best defense. Here's a classic PBX trick, care of the Computer Security Institute: "'Hi, I'm your AT&T rep, I'm stuck on a pole. I need you to punch a bunch of buttons for me.'"

And here's an even better one: "They'll call you in the middle of the night: 'Have you been calling Egypt for the last six hours?' 'No.' And they'll say, 'well, we have a call that's actually active right now, it's on your calling card and it's to Egypt and as a matter of fact, you've got about $2,000 worth of charges from somebody using your card. You're responsible for the $2,000, you have to pay that...' They'll say, 'I'm putting my job on the line by getting rid of this $2,000 charge for you. But you need to read off that AT&T card number and PIN and then I'll get rid of the charge for you.' People fall for it." (Computer Security Institute).

Help desks are particularly vulnerable because they are in place specifically to *help*, a fact that may be exploited by people who are trying to gain illicit information. Help desk employees are trained to be friendly and give out information, so this is a gold mine for social engineering. Most help desk employees are minimally educated in the area of security and get paid peanuts, so they tend to just answer questions and go on to the next phone call. This can create a huge security hole.

The facilitator of a live Computer Security Institute demonstration, neatly illustrated the vulnerability of help desks when he "dialed up a phone company, got transferred around, and reached the help desk. 'Who's the supervisor on duty tonight?' 'Oh, it's Betty.' 'Let me talk to Betty.' [He's transferred.] 'Hi Betty, having a bad day?' 'No, why?...Your systems are down.' She said, 'my systems aren't down, we're running fine.' He said, 'you better sign off.' She signed off. He said, 'now sign on again.' She signed on again. He said, 'we didn't even show a blip, we show no change.' He said, 'sign off again.' She did. 'Betty, I'm going to have to sign on as you here to figure out what's happening with your ID. Let me have your user ID and password.' So this senior supervisor at the Help Desk tells him her user ID and password." Brilliant.

A variation on the phone theme is the pay phone or ATM. Hackers really do shoulder surf and obtain credit card numbers and PINs this way. (It happened to a friend of mine in a large US airport.) People always stand around phone booths at airports, so this is a place to be extra cautious.

Dumpster Diving

Dumpster diving, also known as trashing, is another popular method of social engineering. A huge amount of information can be collected through company dumpsters. The LAN Times listed the following items as potential security leaks in our trash: “company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware.”

These sources can provide a rich vein of information for the hacker. Phone books can give the hackers names and numbers of people to target and impersonate. Organizational charts contain information about people who are in positions of authority within the organization. Memos provide small tidbits of useful information for creating authenticity. Policy manuals show hackers how secure (or insecure) the company really is. Calendars are great – they may tell attackers which employees are out of town at a particular time. System manuals, sensitive data, and other sources of technical information may give hackers the exact keys they need to unlock the network. Finally, outdated hardware, particularly hard drives, can be restored to provide all sorts of useful information. (We’ll discuss how to dispose of all of this in the second installment in this series; suffice it to say, the shredder is a good place to start.)

On-Line Social Engineering

The Internet is fertile ground for social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of one simple password on every account: Yahoo, Travelocity, Gap.com, whatever. So once the hacker has one password, he or she can probably get into multiple accounts. One way in which hackers have been known to obtain this kind of password is through an on-line form: they can send out some sort of sweepstakes information and ask the user to put in a name (including e-mail address – that way, she might even get that person’s corporate account password as well) and password. These forms can be sent by e-mail or through US Mail. US Mail provides a better appearance that the sweepstakes might be a legitimate enterprise.

Another way hackers may obtain information on-line is by pretending to be the network administrator, sending e-mail through the network and asking for a user’s password. This type of social engineering attack doesn’t generally work, because users are generally more aware of hackers when online, but it is something of which to take note. Furthermore, pop-up windows can be installed by hackers to look like part of the network and request that the user reenter his username and password to fix some sort of problem. At this point in time, most users should know not to send passwords in clear text (if at all), but it never hurts to have an occasional reminder of this simple security measure from the System Administrator. Even better, sys admins might want to warn their users against

disclosing their passwords in any fashion other than a face-to-face conversation with a staff member who is known to be authorized and trusted.

E-mail can also be used for more direct means of gaining access to a system. For instance, mail attachments sent from someone of authenticity can carry viruses, worms and Trojan horses. A good example of this was an AOL hack, documented by VIGILANTe: “In that case, the hacker called AOL’s tech support and spoke with the support person for an hour. During the conversation, the hacker mentioned that his car was for sale cheaply. The tech supporter was interested, so the hacker sent an e-mail attachment ‘with a picture of the car’. Instead of a car photo, the mail executed a backdoor exploit that opened a connection out from AOL through the firewall.”

Persuasion

The hackers themselves teach social engineering from a psychological point-of-view, emphasizing how to create the perfect psychological environment for the attack. Basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness. Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of a comfortable relationship.

Impersonation generally means creating some sort of character and playing out the role. The simpler the role, the better. Sometimes this could mean just calling up, saying: “Hi, I’m Joe in MIS and I need your password,” but that doesn’t always work. Other times, the hacker will study a real individual in an organization and wait until that person is out of town to impersonate him over the phone. According to Bernz, a hacker who has written extensively on the subject, they use little boxes to disguise their voices and study speech patterns and org charts. I’d say it’s the least likely type of impersonation attack because it takes the most preparation, but it does happen.

Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a trusted third party (for example, the President’s executive assistant who is calling to say that the President okayed her requesting certain information), or a fellow employee. In a huge company, this is not that hard to do. There is no way to know everyone - IDs can be faked. Most of these roles fall under the category of someone with authority, which leads us to ingratiation. Most employees want to impress the boss, so they will bend over backwards to provide required information to anyone in power.

Conformity is a group-based behavior, but can be used occasionally in the individual setting by convincing the user that everyone else has been giving the

hacker the same information now requested, such as if the hacker is impersonating an IT manager. When hackers attack in such a way as to diffuse the responsibility of the employee giving the password away, that alleviates the stress on the employee.

When in doubt, the best way to obtain information in a social engineering attack is just to be friendly. The idea here is that the average user wants to believe the colleague on the phone and wants to help, so the hacker really only needs to be basically believable. Beyond that, most employees respond in kind, especially to women. Slight flattery or flirtation might even help soften up the target employee to co-operate further, but the smart hacker knows when to stop pulling out information, just before the employee suspects anything odd. A smile, if in person, or a simple “thank you” clenches the deal. And if that’s not enough, the new user routine often works too: “I’m confused, (batting eyelashes) can you help me?”

Reverse Social Engineering

A final, more advanced method of gaining illicit information is known as “reverse social engineering”. This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around. If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees; however, this requires a great deal of preparation, research, and pre-hacking to pull off.

According to Methods of Hacking: Social Engineering, a paper by Rick Nelson, the three parts of reverse social engineering attacks are sabotage, advertising, and assisting. The hacker sabotages a network, causing a problem arise. That hacker then advertises that he is the appropriate contact to fix the problem, and then, when he comes to fix the network problem, he requests certain bits of information from the employees and gets what he really came for. They never know it was a hacker, because their network problem goes away and everyone is happy.

Conclusion

Of course, no social engineering article is complete without mention of Kevin Mitnick, so I’ll conclude with a quote from him from an article in Security Focus: “You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation.” Stay tuned for Part II: Combat Strategies, which will look at ways of combatting attacks by identifying attacks, and by using preventative technology, training, and policies.

To read **Social Engineering, Part Two: Combat Strategies**, click here.

References

Ameritech Consumer Information “Social Engineering Fraud,”
http://www.ameritech.com/content/0,3086,92,00.html

Anonymous “Social engineering: examples and countermeasures from the real-world,” Computer Security Institute
http://www.gocsi.com/soceng.htm

Arthurs, Wendy: “A Proactive Defence to Social Engineering,” SANS Institute, August 2, 2001.
http://www.sans.org/infosecFAQ/social/defence.htm

Berg, Al: “Al Berg Cracking a Social Engineer,” by, LAN Times Nov. 6, 1995.
http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

Bernz 1: “Bernz’s Social Engineering Intro Page”
http://packetstorm.decepticons.org/docs/social-engineering/socintro.html

Bernz 2: “The complete Social Engineering FAQ!”
http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

Harl “People Hacking: The Psychology of Social Engineering” Text of Harl’s Talk at Access All Areas III, March 7, 1997.
http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html

Mitnick, Kevin: “My first RSA Conference,” SecurityFocus, April 30, 2001
http://www.securityfocus.com/news/199

Orr, Chris “Social Engineering: A Backdoor to the Vault,”, SANS Institute, September 5, 2000
http://www.sans.org/infosecFAQ/social/backdoor.htm

Palumbo, John “Social Engineering: What is it, why is so little said about it and what can be done?”, SANS Institute, July 26, 2000
http://www.sans.org/infosecFAQ/social/social.htm

Stevens, George: “Enhancing Defenses Against Social Engineering” SANS Institute, March 26, 2001
http://www.sans.org/infosecFAQ/social/defense_social.htm

Tims, Rick “Social Engineering: Policies and Education a Must” SANS Institute, February 16, 2001
http://www.sans.org/infosecFAQ/social/policies.htm

Verizon “PBX Social Engineering Scam” 2000
http://www.bellatlantic.com/security/fraud/pbx_scam.htm

VIGILANTe “Social Engineering” 2001
http://www.vigilante.com/inetsecurity/socialengineering.htm