SANS | GIAC CERTIFICATIONS

WHITE PAPER

Social Engineering

Aaron Dolan

Social Engineering

Aaron Dolan
GSEC Option 1 version 1.4b
February 10, 2004

Abstract

It's not always what you know, it's who you know. Whether it is a good deal on a product, a free place to stay on a vacation or the extra edge to beat out competition for a job, knowing the right people helps people get the things they want. This 'knowing the right people' is a form of social engineering. Social engineering is using relationships with people to attain a goal. Unfortunately, when it comes to the security of an organization's data and infrastructure, social engineering can be as bad as 'knowing the right people' can be good. This paper will describe social engineering and some of the common techniques used by social engineers. It will suggest policies, standards and procedures for helping to combat such a threat.

Definition

According to Merriam Webster's dictionary, social engineering is the "management of human beings in accordance with their place and function in society, applied social science."[1] "It is the practical application of sociological principles to particular social problems."[2] Social Engineering is essentially using human relationships to attain a goal. It is used by the most effective of law enforcement agencies, such as a local undercover police officer posing as a drug user to arrest a drug dealer, or spies oversees trying to gain intelligence about the next terrorist attack. In this paper, social engineering will be discussed as it applies to the malicious intent of individuals trying to illegally compromise corporate assets.

Some may say that social engineering is an art or a skill that not everyone has. This is partly true as not everyone has good social skills. However, most humans are programmed to be social engineers at a very early age. As children, humans learn how to get what they want by using social engineering tactics. With a little thought and effort, social engineering can be an easy and efficient way for an individual with malicious intent to make life for any organization difficult. Social engineering doesn't require vast technical knowledge, but relies heavily on social skills. A hacker who spends several hours trying to break passwords could save a great deal of time by calling an employee, posing as a helpdesk or IT employee, and asking for it.

Tools of the Trade

Social engineers use tactics to leverage trust, helpfulness, easily attainable information, knowledge of internal processes, authority, technology and any combination there of. They often use several small attacks to put them in the position to reach their final goal. Social engineering is all about taking advantage

[1] *http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=social+engineering*
[2] *The American Heritage® Dictionary of the English Language, Fourth Edition*

of others to gather information and infiltrate an attack. The information gained in a phone book may lead to a phone call. The information gained in the phone call may lead to another phone call. A social engineer builds on each tidbit of information he or she gains to eventually stage a final, deadly attack. A successful social engineering attempt could result in great financial loss for the target company. A motivated attacker will be willing to gain information in any way possible.

Establishing Trust

Human nature is the social engineer's greatest exploit. As part of human nature, people generally trust easily and get satisfaction out of helping those in need. In order to gain information, such as a phone number or a password, the attacker must first establish trust with the individual that he or she hopes to gain information from. Social engineers often use a direct approach to gain the information they need for an attack by simply calling and asking for information. Often the attacker will use a series of calls to multiple individuals to gather the information and/or access needed to cause damage. The social engineer may test the waters with an individual they have contacted by asking simple questions or even making small talk with them. An effective social engineer is very good at picking up on warning signs such as the hesitation of an individual to offer certain information. A sense of hesitation shows the attacker that trust has not been established and that the individual is more likely to catch on or not reveal information.

The easiest way for a social engineer to gain trust is to not ask suspicious questions. A social engineer who asks about sensitive information right off the bat will be less successful than a social engineer who doesn't ask such suspicious questions. This is why social engineers instigate a series of conversations to gain bits and pieces of information at a time. A social engineer will generally start by asking simple questions that seem minute to the attacked. If an attacker senses hesitation in the voice on the other end of the phone, he or she will stick to simple questions and hope to gain more information from the next individual he or she chooses to call. The larger the organization, the easier it is to establish trust. In a smaller environment the target is much more likely to know whether or not the attacker is who they say they are. Trust is important to establish both as a technique on its own as well as in combination with other techniques.

Help

A social engineer may use a tactic known as reverse social engineering. There are three parts to reverse social engineering: "sabotage, advertising and assisting."[3] Reverse social engineering involves creating a situation where the attacker must help the target individual. This is a great way of establishing trust

[3] http://www.securityfocus.com/infocus/1527

because a target individual who gets help from an attacker will be more willing to help the attacker in return. When creating a situation for reverse social engineering, an attacker will generally pose as someone whom the attacked will recognize as an individual who can both solve their problem and receive privileged information. The attacker will try and choose an individual that he or she believes has information to help them. An attacker may make up a situation where nothing even goes wrong to effectively use the reverse approach. An attacker posing as an IT employee, for example, could call and warn the target individual of an outage that may affect their network connectivity. After the false outage window expires, the attacker will follow up with the target to verify they are not having any problems, knowing that the target will not. After creating such a situation, the attacker has established a level of trust that can be used to ask for help in gaining information in the future. This is also a good way for a social engineer to install malicious software on a targets machine. The social engineer posing as an IT employee or software vendor may ask the target to go to a website or open an email attachment sent to the target that may contain a virus or other malicious software. In this situation the social engineer may say, for example, that the software is required to be installed as part of an upgrade.

Easily Attainable Information

Unfortunately, social engineers thrive on easily attainable information such as phone numbers. Social engineers planning to pose as an internal employee will first need to identify someone to masquerade as. Corporate directories are often easy to come by, and not viewed by internal employees as containing sensitive information. Many individuals may think that sharing names, positions and phone numbers is harmless. Cold calling sales people often gain contact information on the people they want to sell their products to from other individuals employed by the same company. Social engineers do this to gain the contact information of the people they want to take advantage of. A call to a corporate receptionist to learn the name and number of a manager, or anyone in a certain position, for that matter, can be quite simple. Social engineers may call the human resources department to learn the names of the employee's they want to target. The attacker may also gather easily attainable information by browsing corporate web sites.

Knowledge of Internal Processes

An attacker can have much success by knowing both internal lingual and business processes. By displaying knowledge of an internal process or procedure or by using internal jargon, a social engineer can trick a target into thinking that he or she is indeed a company employee. For example, knowing the method a helpdesk uses to verify identities and responding as expected will increase the believability of a call to the helpdesk from a social engineer posing as an employee who forgot his or her password. The attacker may already have a good deal of information about the target. A distraught ex-employee wanting to disrupt business likely already knows the key people that he or she can use as pawns for the attack. The ex-employee could also have established some ground work before leaving, such as installing malicious software. For this reason, it is not necessarily outside forces that are most dangerous to an organization's assets being compromised. Rather, it can be an organization's employees themselves.

Clout

Clout, or having authority over an individual, is a technique used by social engineers to intimidate the target. This is often done by posing as an authoritative figure such as a manager. After the social engineer has gained information about the people in charge, he or she may pose as such an individual and call a target demanding information. To use clout effectively, social engineers do not have to necessarily pose as management. They could instead say that they are calling on behalf of a CEO, CFO or other high-ranking official who needs information now and won't take no for an answer. Once the sensitive information is revealed, trust is also established, meaning that the attacker could use this approach against the same person again in the future.

Technology

Although a successful social engineering attack does not require a great deal of technical knowledge, using technology in conjunction with social engineering principals can be very effective. A social engineer may use the techniques above to learn about the technical infrastructure of a corporation in order to unleash a virus that could potentially take down a network. Social engineers may deploy a "Trojan horse, a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage."[4]

> A social engineer may send a virus or Trojan horse as an email attachment; capture victim keystrokes with expendable computer systems or programs; leave a floppy disk or CD around the workplace with malicious software on it; use false pop-up window's asking a user to log in again or sign on with their network password; send free software or a patch for a victim to install. [5]

Gaining Physical Access

Many corporate offices hold a lot of easily attainable information that can help a social engineer perpetrate his or her attack. Although social engineers tend to avoid going on site of a target, doing so can be easy. These days, most large organizations use a badging system for getting in to a building or secured area.

[4] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html
[5] Mitnick, P. 332

Being that humans are generally polite, following someone in to a corporate office can be very simple. At large organizations most employees do not know every employee or recognize every face and are usually more than happy to hold a door for someone. Once in, the social engineer can gain a great deal of information from just walking by the workspaces of employees who have stepped away. From taking a walk through a corporate office, a social engineer may find passwords on sticky notes stuck to monitors, financial records such as invoices and purchase orders, or documentation on the technical infrastructure. The attacker can leave with such information in hand.

Being on site is most advantageous after hours. Social engineers may pose as cleaners or maintenance workers to get in after hours. Some may even get a job with a contracted cleaning company to get inside the target. Once on site after hours, a social engineer may find a workstation of someone who hasn't logged out or locked their workstation, and install malicious software or steal information. The attacker may find sensitive information that was not properly destroyed. He or she could install networking equipment such as wireless access points. A social engineer that goes inside the target company is going to be as quick and stealthy as possible, but at night when no one is around he or she can let down their guard a bit more and take more time gathering information. A social engineer in the office undetected after several hours can easily steal hardware and software or anything else he or she feels may help in reaching the final goal.

Defending Against Social Engineering

How does a company defend against social engineering? Successful social engineering attacks rely on the employees of an organization. To contain such an attack, employees must be well trained and familiar with common social engineering techniques. It is also important for organizations to establish a clear and strong security policy, including standards, processes and procedures to help eliminate the threat of social engineering. A good social engineering defense should include but not be limited to:

- Password policies
- Vulnerability assessments
- Data classification
- Acceptable use policy
- Background checks
- Termination process
- Incident response
- Physical security
- Security awareness training

Password Policies and Standards

For a social engineer, gaining access to a system can mean the difference between a successful or failed attack. A policy should exist for the delivery and creation of passwords. A good password policy should include information about:

- Not sharing passwords when asked
- Not writing down passwords
- Not using default passwords
- Methods for identifying users for password resets
- Methods for password delivery
- Password creation i.e. minimum length, alpha-numeric
- Securing workstation with a password protected screen saver when before leaving a workspace
- Periodic password change
- Grace period for expiring passwords
- Login failure lockout i.e. account is locked after 3 failed attempts
- Administrative and System password standards

Employees must realize the importance of a strong password. Using any word found in a dictionary, or combination there of should not be allowed. Controlling this can be difficult as more and more systems are implemented, there are more and more passwords to remember. Tools can be implemented, such as password change applications, to help ensure employees choose a proper password. Having a strong password is extremely important in any environment in particular environments using single sign-on technologies. Single sign-on allows users to use one password to access a wide range of network resources. Although these systems can help diminish the stress of remembering multiple passwords, it also means that there is only one password to crack.

Social engineers using the physical approach to gain information can often attain passwords by simply strolling past workspaces. The invention of the sticky note has proved to be a headache for security professionals as well as a blessing to social engineers. It is too common for individuals to write down passwords on sticky notes and post them on their monitor or other easy to see location. Other employees may consider hiding passwords under their mouse pads as appropriate. Unfortunately, most organizations don't allocate resources to essentially hold the hands of employees to make sure passwords are not being written down and posted. A good password policy should require that employees do not write down passwords.

Although policies are written to be followed and should require employee sign off, taking the time to track down offenders can be costly and time consuming. A policy is no good if it is not enforced, which is why training is extremely important and required to ensure such a policy is followed. If an employee truly understands the risks involved in writing down and posting passwords as well as sharing sensitive information, he or she will be less likely to do so. Employees must take an active role in their organization's security. An understanding of the risks and consequences of their actions must be driven home to help combat social engineering.

An organization's helpdesk and IT staff must follow a strict identity verification and password delivery policy. Identity verification, in this case, refers to authenticating that a caller is indeed the individual they claim to be. System administrators need a way to validate the individual they are communicating with. In today's world, recognizing a voice is not a sufficient mechanism for identity verification. Then there is the issue of someone having the ability to change a password in general. A disgruntled helpdesk employee or system administrator that can change passwords could steal information and cause major problems for an organization. To help combat this, the burden of identifying individuals for password resets can be shifted away from a helpdesk. With self service password change technologies, a human does not have to validate that another human is indeed who they say they are. Challenge response technologies are becoming more and more popular and widely used across enterprise environments. With challenge response, a user is required to answer a question or multiple questions before being given the ability to change their own password via a web interface.

There are many suggestions out there on proper password delivery. For example, some organizations may insist that passwords be delivered by intra-company mail or other courier service. This means that passwords are written down and can be intercepted. Some organizations validate an employee by using caller ID. The premise here, in the event of a password change, is to call back an individual at the number appearing on the caller ID to validate identity. Such a method is insecure as someone making a call from Bob's workspace may not actually be Bob. Other organizations validate account owners by asking for personal information such as a social security number. This relies on the storage of employee information in a manner that could be accessed by personnel who may share it with an attacker or use it themselves. The point here is that most password delivery methods are not 100% fail safe. If passwords are delivered on paper, via electronic or snail mail, the login ID and system information should never be revealed.

If email is not an appropriate means for a company to communicate passwords, it could instead be used to let the account owner know that a request to change a password has been made. For example, an organization is using a password self service application could have the system send an automated email to the account owner, or authoritative figure stating that an account's password has been changed. The automated email could include the date and time the change was made and the IP address of the machine where the change was made. If an automated email feature is not suitable, logging should be enabled to track password changes.

Another consideration when creating a proper identity verification and password delivery method is the type of account being updated. An administrative account for a system containing a plethora of confidential information may need to follow an entirely separate process for delivery, creation and changing of the password. This is why it is important to create separate policies for accounts based on the account type. A separate policy should exist for administrative and user accounts. A separate password standard may also be needed per account type. An administrative password or root account password to a system such as a firewall may need to be longer in character length and use different naming conventions for the login ID than that of a user's network password.

Vulnerability Assessments

Be it external or internally provided, organizations should implement periodic penetration and vulnerability assessments. Such assessments usually consist of using known hacker tools and common hacker techniques to compromise a network. Adding social engineering is essential to providing an accurate assessment. Since such an attack takes advantage of employees, using social engineering as part of a penetration test may have legal implications and as such, should be clearly defined and approved before occurring.

Data Classification

Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees are aware of and adhere to. Data classification assigns a level of sensitivity to company information. Each level of data classification includes different rules as to who can view it, who can edit it and if/how it can be shared. Data classification helps to deter social engineering by providing employees a mechanism for understanding what information can be disclosed. Data classification also helps to ensure the integrity of data as, depending on classification, documents should be assigned an owner or sole party responsible for updating such documents. The following is an example of a data classification model:

> Top Secret: Highly sensitive internal documents e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
>
> Highly Confidential: Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of

bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

Proprietary: Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level is high.

Internal Use Only: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

Public Documents: Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.[6]

The above uses terms for the security of the data as: high as possible, very high, high, controlled and minimal. The way that data is protected should be based on the type of classification the data is given. Because of this, it is important to include data classification as part of an application development or roll out plan. The way that top secret information is stored and protected will vary from the way public documents are protected. Top secret information may be contained within a DMZ behind firewalls that only allow specific clients to access the hosts containing the data, while public documents may be readily available for anyone to view on an external website. It is also important to have defined methods for the destruction of top secret, confidential, proprietary and internal documents.

There are other data classification models that can be found on the internet, each of which may use different language for data classification i.e. using the term classified instead of confidential. SANS' offers an Information Sensitivity template which can be found at: http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf. Having a data classification model in place will help deter social engineers from attaining information easily, as well as enable employees to know whether or not the data any individual is asking for should be disclosed.

Acceptable Use Policy

An acceptable use policy also helps ensure that confidential data is not shared and that systems are not misused. Such a policy includes information about how

[6] http://www.yourwindow.to/information-security/gl_dataclassification.htm

an information system shall be used, to help ensure that systems are only used for their intended purpose. An acceptable use policy should include information on the following:

- Information systems and network resources are provided for authorized use only
- Providing authentication credentials to unauthorized users is prohibited
- Confidential information may not be released to any third parties
- Unacceptable e-mail usage
- Harassment
- Forgery/misrepresentation
- Attempting to gain access to unauthorized resources
- Commercial use of information resources
- Abuse of internet connectivity
- Denial of service
- Unauthorized/illegal software
- Use of networks in violation of federal, state or local laws[7]

Background Checks

Social engineers will use any method possible to attain their goal. Although the most common social engineering attacks use insiders indirectly, it is not entirely uncommon for an attacker to get on the inside of a target by becoming employed by the target company. Background checks are important to businesses in general and are an essential part of the defense against social engineering. Background checks should not be limited to internal employees. Vendors, interns, and contractor/temporary workers should also be cleared before access is granted to enter the premises or connect to the company network remotely. It is important for corporations to understand what types of background checks are done on employees of contracted companies. A company may have an outstanding background check process for internal employees but may be unaware of the kind of checks performed on contracted staff such as outsourced cleaning crews. Simply verifying background checks are done is not enough. Organizations should be aware of the type and strictness of the background checks performed. A good background check may include:

- Nationwide criminal record search.
- Current and previous address summary.
- Drug screening
- Motor vehicle report
- Civil court history
- Criminal court history
- Federal court history
- Credit checks

[7] Mandia & Prosise P.463-464

- Education Verification
- Personal References check
- Worker's compensation report[8]

The types of background checks used will vary from organization to organization as well as within an organization. A motor vehicle report may not be required for applicants not using company vehicles for example. Having strong background checks can help ensure that a malicious individual does not become employed by an organization, in turn deterring social engineering attacks.

Termination Process

An effective termination process is a must for deterring terminated employees from using their access to information and physical assets to cause damage to the organization. For the purposes of this paper, termination refers to the termination of access to information and physical assets, and should occur when an employee quits, is fired, laid off or takes a leave of absence. A process for terminating access should include the immediate removal of network access, remote access, access to facilities, and all access to applications used by the employee. When an employee is fired, his or her access should be terminated at the same time he or she is given word of the termination of employment. Although organizations may not want to terminate access before an employee is escorted out of the building, a coordinated effort needs to be in place between human resources, the employee's manager, information security and physical security personnel. When an employee takes a short term leave of absence a process for short term termination of access should exist. Locking accounts vs. removing accounts makes sure the employee cannot do damage while also allowing for less headache when the employee returns.

When it comes to system administrators, extra steps must be taken to ensure that all access to information systems is removed. All administrative passwords that the employee has knowledge of must be changed immediately. It may require that other administrators halt their other activities, but it is a necessary action to help reduce the likelihood of a successful attack on the corporate network. Having a termination process in place that is efficient will help corporations defend against attacks conducted by disgruntled ex-employees attempting to use internal knowledge.

Incident Response

In the unfortunate event that an attack occurs an incident response process must be in place to help contain and gather information about an attack. An attack that goes unnoticed may just be the beginning of a string of attacks. Identifying and dealing with an attack in an efficient manner is important to deterring future attacks as well as containing an incident. Incident response plans will vary

[8] http://www.bcint.com/services.html

widely from organization to organization. It is important to have an incident response process designed specifically for an organization to deal with information gathering and analysis of malicious events. In the case of social engineering, employees should have a phone number or contact person to go to immediately after discovering that an incident has happened or is under way. Employees should be encouraged to report any unusual activity he or she witnesses including phone calls.

"By centralizing the reporting of suspected security incidents, an attack that may otherwise have gone unnoticed can be detected. In the event that systematic attacks across the organization are detected and reported, the incident reporting organization may be able to determine what the attacker is targeting so that special efforts can be made to protect those assets."[9]

Physical Security

Having effective physical security measures will help minimize the entering of a facility by a social engineer. There are some basic principals that can be implemented which can greatly reduce the threat of a physical breach:

> Identification for nonemployees: Individuals that need to enter company premises on a regular basis should be issued a special form of identification. Individuals making deliveries, stocking vending machines, ATM vendor's, and amenity related individuals such as dry cleaning pick up should be issued unique identification credentials.
>
> Visitor Identification: Visitors should be required to present physical identification such as a driver's license as well as sign a log including the time of arrival their contact at the company and when they plan to leave. Comparing a signature as well as a face with the driver's license signature/picture can help physical security staff determine that the individual is who they claim to be. The driver's license should be photocopied and kept while the visitor is on site and retained for a period of time in case an incident is reported after the visitor has left. After proper ID verification the visitor should be issued a temporary badge that expires at the time the visitor has indicated they will be leaving.
>
> Escorting visitors: Once given a visitor identification badge, no visitor should be allowed to enter the premises without first being assigned a responsible employee. The visitor should be escorted by this employee at all times while on site.
>
> Temporary Badges: Employees that have forgotten their badge should be issued a temporary badge after the employee's identity has been verified. The supervisor of the employee should be notified via email that a

[9] Mitnick, P. 282

temporary badge was issued for to the employee for the day. All temporary badges should be logged and turned in at the end of the day, if not turned in, the badge should be disabled by the physical security employees.

Vehicle license plate numbers: If there is a guarded parking lot or garage, license plates of all vehicles entering the area should be logged by security staff.

Trash dumpsters: Trash dumpsters should not be accessible to the public. They should instead be stored in a secured area so that individuals cannot dig through them to find confidential information that was not properly destroyed. This practice of digging through dumpsters to find information is known as dumpster diving.[10]

Security Awareness Training

The most important part of an effective security policy is making sure all employees are aware and adhere to it. All employees should be required to attend security awareness training periodically. Depending on the environment, it may be a good practice to require security awareness training annually. New hires should be required to read all security policies as well as sign a document acknowledging that they have read, understand and agree to abide by the policies.

A good security awareness training program will include information on all security policies, and include education on social engineering techniques. Employees should be given information on who to call when a suspicious event happens. They must be given an understanding of their responsibility in keeping an organization's data and infrastructure secure. Security awareness training could mean the difference between a social engineering attack being successful or not. Employees who are aware of security and what it means to them and their employer will also be less offended when a fellow employee does not hold a door for them or questions their identity during a phone conversation. A proper awareness program is essential to help combat social engineering.

Conclusion

Social engineering can be a very effective and dangerous method for individuals to compromise both information and infrastructure. Social engineering is unlike any other threat to the security of a corporation. Social engineering bypasses the technologies put in to place to protect and detect malicious activity. It is a threat that will always exist, and one that cannot be contained by anti-virus software, thorough patching, firewalls and intrusion detection systems. It only takes one unaware employee to make a social engineering attack successful, and as a

[10] Mitnick, p. 324-326

result makes employees the weak link to a security policy. With the proper training, and policies in place, the risk of social engineering can be effectively mitigated.

Bibliography

Merriam-Webster Online (http://www.m-w.com) Merriam-Webster INC. 2004 URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=social+engineering

The American Heritage® Dictionary of the English Language, Fourth Edition Houghton Mifflin, 2000.

Granger, Sarah "Social Engineering Fundamentals, Part I: Hacker Tactics" December 18, 2001 URL: http://www.securityfocus.com/infocus/1527

searchSecurity.com Definitions, whatis.com 2004
URL http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html

Mitnick, Kevin and Simon, William L. The Art of Deception Wiley Publishing 2002

Information Security Policy and Disaster Recovery Associates, UK URL: http://www.yourwindow.to/information-security/gl_dataclassification.htm.

Mandia, Kevin & Prosise Chris Incident Response McGraw-Hill 2001.

Background Check International, LLC. URL: http://www.bcint.com/services.html

Wilson, Sam "Combating the Lazy User: An Examination of Various Password Policies and Guidelines" Sept. 16, 2002. URL: http://www.sans.org/rr/papers/6/142.pdf

Smith, Richard E. Authentication: From Passwords to Public Keys Addison Wesley, 2002