Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Proactive Defence to Social Engineering

Companies spend a lot of time and money trying to protect their networks. Most of their attention focuses on technology such as upgrades, security kits and high-end encryption. However, a popular means of gaining access bypasses the technical systems completely and is based on the long-time con or confidence game with a new name and new face - social engineering. A company needs good policies in place to defend against this type of attack, but even more, they need an effective, on-going security awareness program. The ...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

A Proactive Defence to Social Engineering

Introduction

Intruders or hackers are continually trying to gain illicit access to computer systems and there are many different types of attack. Companies spend a lot of time and money trying to protect their networks. Most of their attention focuses on technology such as upgrades, security kits and high-end encryption but a popular means of gaining access bypasses the technical systems completely. It's based on the long-time con or confidence game but has a new name and new face – social engineering. A company needs good policies in place to defend against this type of attack, but even more, they need an effective, on-going security awareness program. The best means of defence, in this case, is education.

Why Social Engineering?

Social engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software present. It's the hardest form of attack to defend against because hardware and software alone won't stop it.

Social engineering has been around as long as man. It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system – the human being. Social engineers are con artists who exploit human vulnerabilities such as ignorance, naiveté and an individual's natural desire to be liked and helpful.

Methods of Attack

Social engineering can be described in terms of two main categories, human based attack and computer based attack. Computer based social engineering relies on technology to trick the individual into supplying information which will allow the hacker to gain further access into the network. For instance, a pop-up window may be used, telling the user that his network connection was lost and that he needs to re-enter his user name and password to reconnect. Once done, the information is emailed back to a remote site by a program that the intruder had already installed. This requires the intruder to have already gained a certain level of access to the system.

The simplest and most popular means of social engineering is still human based. It relies on interpersonal relations and deception, using the 'tools' of the trade such as flattery, intimidation, name-dropping, asserting authority and belittling. "Any medium that provides one-to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar." (Dorothy E. Denning, *Information Warfare and Security*)

A good social engineer will do a bit of background research on the target company to get an idea of the basic structure and even some names. This can be as simple as walking into the company building and reading the building roster. The roster quite often has a wealth of information such as the department names and sometimes even the names of the department

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

heads. Another classic means of collecting information is "dumpster diving", this refers to the analysis of the contents from a target's trash bins. Stealing trash is not illegal. The Supreme Court ruled in 1988 that once an item is left for trash pickup, there is no expectation of privacy or continued ownership. (Richards J. Heuer, Jr, *Theft and "Dumpster Diving"*)

Once the intruder has acquired some basic information, he can begin phoning different departments within the target organization to gain more specific information. Social engineering usually involves some form of impersonation, of either a particular individual or a role. The person may pretend to be a repairman, a fellow employee, a manager or a person of trust phoning with the authority of an important user. For example:

- Repairman - How many times have you seen a telephone repairman working on a phone in your building? Most people accept either a telephone repairman or computer technician without challenging them. The act of snooping around for that password hidden under the phone, keyboard or desk blotter appears as though it's a normal activity performed during the course of his duties.

- IT Support – Somebody, claiming to be from the company's IT support group, phones a user and explains that he is fault finding on the network. He has limited the fault to within the users department but he needs a user ID and password from that department to finish tracing the problem. Unless the user has been properly educated in security practices, he will very likely give the "trouble-shooter" his information.

- Fellow Employee – A man dressed in a suit with a rather harried expression on his face walks into a room full of workers. He says he just started working for the company but he's forgotten the password to the finance database, asks if, anyone can remind him? Chances are that at least one person will tell him.

- Manager – The social engineer, using a perceived position of authority, phones the help desk demanding to know why he can't log on with his password. He then intimidates the help desk into giving him a new password by telling them he only has a limited time to retrieve some information for a report to the company vice-president. He may also threaten to report the help desk employee to his supervisor.

- Trusted Third Party – The social engineer phones the help desk, claiming to be Susan Sly, the vice-president's executive assistant, stating the vice-president has authorized her to collect the information. If the help desk employee balks, she threatens job loss or a report to the employee's supervisor.

Help Desks can be particularly vulnerable to social engineering because they are the first line of support for problems on the network.

Policies

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Good policies are one of the essential cornerstones to a security program. They should be written with the target audience in mind. In other words, policies should be written in a clear, concise language, devoid of IT jargon. They should also describe what is expected and identify who to contact if any questions arise.

Policies have a life span of their own and should have a review date, as they need to be kept current. To keep the process manageable, policies should, as a rule of thumb, be reviewed, on a rotational basis, at least every five years, with 20% of the policies under review each year. More volatile policies may be reviewed more frequently, and as issues arise policies may be redrafted or modified to suit changing requirements and technologies. In that way, old policies can be updated, obsolete policies can be cleared out and new requirements blended into a living document. Once updated, the policies can be posted on the company's intranet, with current version number and date, so that the current version is always readily available.

Policies that can be put in place to defend against social engineering are:

- Information Release – The security policy should detail who can release information to the public and under what circumstances. For instance, a good policy would refer all surveys to a designated person.

- Access Approval – The security policy should determine:
    - If a security agreement needs to be signed before access is granted,
    - Who has the authority to grant access to the system and what type of access they can give,
    - Decide the methods used to create accounts and terminate accounts; and,
    - Develop specific procedures to create accounts to prevent confusion and reduce mistakes.

- Password Changes – The policy should require the use of special characters, numbers, upper and lower characters to strengthen passwords. It should also state the frequency that passwords must be changed, making sure to strike a balance or the employee will defeat the system by writing down the password

.

- Modems – The policy should clearly state that modems are not permitted on the company intranet as they bypass any firewall the company may have, leaving an open door. An adjunct to the policy would allow the IT security staff to audit for modems on a frequent basis.

- Help Desk – There should be a policy which prohibits the help desk from giving out passwords or other information without first verifying the employee by:
    - Calling the employee back to verify location;
    - Using a caller ID system on the phone;
    - Employee digital signature, for email; or,
    - The employee picking the information up in person.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Employee ID – The organization can develop a policy and procedure to identify employees such as wearing a picture ID card. Visitors would be required to register and wear a temporary ID card. The employees should be encouraged to challenge anyone without a card.

- Shredding – The policy should require any sensitive document to be shredded to avoid the "dumpster diving" scenario.

- Physical Security – Sensitive areas should be identified and kept locked, allowing access only to those with a legitimate need.

- Violations – There should be an easy to use, well-publicized process that employees can use to report any violations of policy or suspicious activity.

- Life Cycling - Information System Life Cycle policies relating to the destruction/storage of both the data and hardware it's stored on should be clearly laid out.

Security Awareness Program

The company security policies have been written and published on the company intranet. An email has been sent to the departmental managers telling them where to find the policies and that all employees are to sign the attached form stating that they have read and understood them. That's all it takes, right? Wrong. That's just the beginning. The most dangerous situation for an organization is when management is deceived into thinking that security controls are in place simply because they are specified in the standards.

There are many tools that can be used in a security awareness program, all curiously effective to a degree. Many organizations use some combination of the following: videos, newsletters, brochures, booklets, signs, posters, coffee mugs, pens and pencils, printed computer mouse pads, screensaver, logon banners, note pads, desktop artefacts, tee shirts and stickers. The biggest problem with things like logon banners, posters and screen savers is that the only way for them to remain even slightly effective is to change them frequently. Otherwise, it's like the advertising sign on the side of the highway the driver passes every day on his way to work. If it's not changed regularly, he doesn't even remember there is a sign.

A security awareness and training program can serve to inform employees about their organization's information security policy, to sensitize them to risks and potential losses, and to train them to recognize social engineering techniques. But it's not enough to tell users how to behave; they must understand and appreciate the reasons behind the rules. The users, whether management or line workers, must buy-in to the program. One effective method is to personalize security concerns, show that 'what they do, how they do it and why they do it' applies to them personally as well as to their company. A major reason for the lack of threat awareness by people is the failure to grasp what can be lost through security breaches. (John D. Johnson, *Infosec for Dummies Part II*)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Although educating employees about the risks of social engineering should be your first line of defence, it may prove to be a daunting task. Everyone is vulnerable to exploitation by social engineers but no one likes to be told their gullible or worse, stupid. One of the best methods for educating employees to these risks is to take social engineering stories from current events and post them on an internal web site, or use email for safety tips and informational stories. The security officer can also incorporate these stories into security awareness training sessions held for employees. The stories work like fables of yore, imparting information with a purpose. Telling authentic stories of what happened to the 'other poor guy' increases resistance to these exploits in a non-threatening way, inoculating the employee against a vulnerability to social engineering.

A good security awareness program must be multi-pronged. The security officer has to use every opportunity and tool in his bag of tricks to ensure that the employee is not only aware of the need for security but understands why as well.

Summary

Social engineering is a serious problem. A company must not only establish good policies to guard against it, but must have an effective security awareness program to communicate those policies. The program should not just reiterate the policies but educate the users to the methods used by social engineers and the risks involved if they succeed. As one of the major points of vulnerability is people, education is an important factor.

References

Donn B. Parker, *Fighting Computer Crime – A New Framework for Protecting Information*, Wiley Computer Publishing

Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley

Lars Klander, *Hacker Proof – The Ultimate Guide to Network Security*, Jamsa Press

Micki Krause, Harold F. Tipton (Editors), *Handbook of Information Security Management 1999*, Auerbach

Author Unknown, *Crime, Security, and Privacy*, University of Memphis, URL: http://www.msci.memphis.edu/~ryburnp/cl/cis/crime.html

Rick Tims, *Social Engineering: Policies and Education a Must*, SANS Institute URL: http://www.sans.org/infosecFAQ/social/policies.htm

Rick Nelson, *Methods of: Social Engineering*, URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html

Richards J. Heuer, Jr, *Theft and "Dumpster Diving"*, URL: http://www.mbay.net/~heuer/T3method/Theft.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**