Social Engineering

What is Social engineering?

In an information security context, social engineering is the art and science of exploiting a person's inclination to trust what they are told and help when they can in order to trick them into providing confidential information that they otherwise would not.

Usually we blindly accept a person, and what they tell us, at face value. We also tend to believe that a scenario is what it appears to be. So when we receive a phone call from "tech support" asking for information about our computer, we tend to believe they are who they say they say they are and that we should provide whatever information is requested. When a close friend sends an email asking for the combination code to our home, which they have forgotten, we tend to believe that the email is actually from our friend, and that they have some legitimate reason to need in our house.

This makes social engineering a much higher risk than typically imagined. In the corporate world we may have installed firewalls, intrusion detection systems, virus scanners and have a group of well trained technicians in place to protect our systems, but a couple of well placed questions or emails can negate all of those efforts and allow an attacker to fully compromise our systems.

The media portrays computer hackers as using sophisticated programs when attacking a computer system. However, is it usually much easier and faster simply to call a person on the phone or send them an email that tricks them into providing the information necessary to compromise a computer system.

When seasoned computer techs read or hear about social engineering, it is always in the context of “don’t let this happen to you!” However, there is a second and equally important perspective to consider – when some other staff member falls victim to a social engineering attack, tech support staff may be the first to recognize the issue. Indications can include excessive and/or unusual:

- CPU utilization
- use of disk space
- disk activity regardless of the amount of free space
- network activity or errors
- Recently installed software
- Errors in the Windows event logs
- Errors in the *nix dmesg log

- Unexpected reboots

- Problems that seem to require a reboot

In information security, we have:

- hardware, the physical pieces you can touch
- software, the virtual 1's and 0's of code
- firmware, the persistent software in memory that is not frequently altered
- and finally we have wetware, the people who use and support the hardware, software, and firmware.

Examples of social engineering attacks

An attacker will ask if you have a particular version of software installed such as a pdf reader, web browser, or operating system. With that information they can email the target an attached file that contains exploit code specifically designed for that particular piece of software. They may ask about the software version couched in a discussion about sending something the person would want - such as the chance to sign up for a drawing for something the person would likely want, or information about a topic the person is very interested it and likely to open.

Once an attacker has compromised someone's email account they can send email to the people on the compromised contact list. Pretending to be the trusted person, they send malware, a malicious link, or malicious attached files or try to illicit information that can be used to further an attack.

A social engineering attack usually includes an enticement. Enticements are anything that leads a person to take some action in return for a promised reward. For example; "wining a prize" or "getting a great deal".

Another example is receiving a response to a question you never asked. Emails with subjects like "You have been approved...", "The info you requested", or "Per our conversation" that come out of the blue. These types of subjects are intended to get you to open the email and possible take some action such as open a hyperlink. In either case, the attacker really wants you to open the email to give the malicious payload the chance to attack.

Defenses

Wither on the phone, in email, or in social media communities get into the habit of thinking before acting. Attackers know that what they are doing should raise a red flag in a person's mind, so they include enticements in order to motivate you to act before considering how much sense the situation actually makes. If you feel rushed, something is wrong!

Be suspicious of anything unexpected or unsolicited. If it is unusual, verify the facts before acting.

No one legitimately asks for passwords, account names, or similar information. Those who have a legitimate and authorized need for any type of confidential or sensitive information will already have an established process to get it - and asking you is never legitimate or authorized! No one, including tech support needs to verify anything. And if there is a chance that they are on the up-and-up, get their name and department and then call your tech support helpdesk to verify that the caller is who they say they are.

One very important piece of defense is an organization's policies. Remember that people usually want to cooperate, answer questions, share information, and be helpful. However, if a policy is in place and the staff have been clearly educated about the policy, they will be much more comfortable, and actually obligated, to not cooperating "because it is against our policy."

References

What is Social Engineering?
Updated: 03 Nov 2010
http://www.webroot.com/En_US/consumer/tips/secure-what-is-social-engineering

Social Engineering Fundamentals, Part I: Hacker Tactics
http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Social Engineering Fundamentals, Part II: Combat Strategies
Updated: 03 Nov 2010
http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies