Global Information Assurance Certification Paper

Information Systems Security User Awareness: Social Engineering and Malware
William Rybczynski
18 November 2000

"Always remember: amateurs hack systems, professionals hack people."

- Bruce Schneier, CTO, Counterpane Internet Security, Inc. Dec 2000

Introduction

As System Administrators and Information System Security Professionals we are tasked with ensuring that the network is available, operational, and that the integrity of the network is secure. Many system administrators and network security personnel are focused on the great technology that is available to us to help shore up our defenses. We employ firewalls and routers with restrictive access lists knowing the technology will help us to secure the perimeter of the network. We use intrusion detection systems and run vulnerability assessments against our networks as often as possible to maintain the integrity of the network. Meanwhile, our users go about their daily jobs. They are creating and sharing files and sending and receiving e-mails. They are surfing the web trying to gather important information to accomplish their assigned tasks. Often times they are downloading freeware and shareware programs that promise to help make their jobs easier. They are dedicated to their jobs. So much so that they dial into the networks from home just to work on important documents during their weekends and holidays. To combat some of these threats the security professionals do their best to ensure that anti-virus programs are installed throughout the network and monitor Internet activity as much as possible. Technology however is not the key. I believe that user awareness is the key that, will help use maintain the integrity of our information systems.

As IS security professionals, we can have a far greater impact on the security of our networks by helping our users to understand the importance of maintaining a high security posture both at work and at home. I will focus on two areas that should be addressed when creating a user awareness program: social engineering and malware.

Social Engineering & Malware

Social engineering is a term most often used among crackers and hackers where the aim is to trick people into revealing passwords or other information that compromises a target system's security.[1] In his book "Secrets and Lies", Bruce Schneier lists social engineering as one of his six "aspects of the human problem" when focusing on information systems security. He states that social engineering is "very effective: and that it goes straight to the "weakest link in any security system: the poor human being trying to get his job done, and wanting to help out if he can." Often times our users are aware of social engineering when they consider phone calls that ask for their passwords. When Kevin Mitnick testified before Congress he told them that he was often able to get the information he wanted simply by pretending to be someone else and asking the unsuspecting user for that information.[2]

Malware is a generic term for viruses, worms, Trojan horses and malicious applets.[3] Most users are aware of the different components of malware, but when someone combines Malware and social engineering the threat increases exponentially.

A popular socially engineered malware attack was the ILOVEYOU worm. Although this attack did not reveal any passwords or security information, it did "trick" the users by "pretending" to be from someone else. Many variants of this worm are still circulating and the worm's author's creativity was in the subject line. The author used social engineering to make users believe that they were receiving a love note from someone else. There are several steps that can be taken to help mitigate these types of threats in the future.

Mitigation Steps

1. Ensure anti-virus software is installed and functioning properly on all user computers and on the mail servers. I know that this seems to be a basic step and it is. The companion piece to this step is the user awareness. Ensure that the users understand that by disabling their anti-virus software on either their work or home computers, if the dial-in, they are not only putting that computer at risk, but the entire network. The Department of Defense understands the risk that malware poses and has licensed several anti-virus products for it's members use on their home computers. Several agencies send out weekly computer security tips and always remind users that they can obtain this free software.

2. Establish policy that states that the users must contact the organization's network security office if they note an anomalous activity on the computer. Again, this is a good standing policy, but it has to be backed up with action from the network security personnel. Establishing open lines of communication between the users and the network security personnel allows the users to call without fear of incrimination. Often times users will either ignore strange activity on their systems or they will fail to contact the appropriate personnel because of the actions that might be taken against them. The security personnel need to help the users understand that malware incidents do occur on the network.

3. Educate the users to be suspicious of anything they receive that asks them to take part in any test programs or that sounds "too good to be true." Instruct them to contact the network security office for clarification before acting on any instructions in the message.[4] It is only a matter of time before some of the infamous chain e-mails in circulation (i.e. the Microsoft/AOL beta e-mail tracking system) start to carry a malware attachment. Users often receive "virus alerts" from family and friends who are only trying to pass along "important information" and they then want to be helpful by passing the information to co-workers. This socially engineered attack can result in a denial-of-service. Many of these types of threats can be stopped if the users have open communications with the network security personnel.

Conclusion

The reality is that social engineering does work and there will always be some new malware, but the threat that social engineering and malware poses to our organization's information systems can be reduced. As these and other threats continue to mount, the IS Security Professional needs to take advantage of every tool available to him. Many technologies are available to assist in this area, but the key component to ensuring the integrity of our information systems is the user. The user is first line of defense and it is his individual security posture that will be instrumental in helping to mitigate future threats. The IS Security Professional can ensure that through effective user awareness training and open communication the individual user understands the great impact he can have on the integrity of the organization's information systems.

References

1. Howe, Dennis. Editor. "The Free On-line Dictionary of Computing" URL: http://foldoc.doc.ic.ac.uk

2. Associated Press. "Guard Passwords, Hacker Says" URL: http://digitalmass.boston.com/news/daily/03/03/mitnick.html

3. Kerby, Fred. "Malicious Software (Malware)" SANS GIAC LevelOne, Security Essentials URL: http://www.sans.org

4. CERT Advisory CA-1991-04 Social Engineering URL: http://www.cert.org/advisories/CA-1991-04.html