Impact of social engineering assignment

Sociology

Impact of Social Engineering Topic: The Impact of Social Engineering I. Introduction A. Definition of Social Engineering B. The goal of Social Engineering C. Reverse Social Engineering II. Body D. Categories of Social Engineering 1. Technology based 2. Non-Technology based E. Types of Social Engineering attacks III. Conclusion F. Defense against Social Engineering G. Impact of a Social Engineering attack Introduction Social engineering has become the most popular method of compromising the security of personal data.

The successful use of Social Engineering techniques has provided attackers and hackers the ability to breach computer systems and gain access to sensitive data. Many computer hackers such as renowned hacker Kevin Mitnick have found that it is easier to trick somebody into giving his or her password than to carry out an elaborate hacking attempt (Mitnick and Simon, 2002). What is social engineering? Social engineering is the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques (Godchild. 2011)”.

Social engineering involves the use of manipulation to trick others into revealing and or providing the needed information that can be used to steal data and or gain access to secured systems. Most victims of social engineering attacks never see their attackers and they seldom realize that they have been hacked or manipulated. The goal of social engineering The main goal or focus of social engineering is to use human weakness to gain access to secure systems and or data. Despite the implementation of a wide range of security controls and measures into a secured system; there will always be a human linked to the system.

Humans are the weakest link in all secured systems. “ Securing the hardware, software, and firmware is relatively easy; it is the “ wetware” that causes the biggest headache” (Peltier, 2006). Wet- ware is defined as the human brain or a human being considered especially with respect to human logical and computational capabilities. What is a reverse social engineering? Reverse social engineering is a more advanced method that hacker may use for the purpose of gaining secured information.

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. ” (Granger, 2001) Reverse social engineering occurs when an attacker convinces their target that he or she has a technical problem and the attacker then helps solve or fix the targets problem.

Reverse social engineering usually begins, with the attacker accessing and damaging the target’s equipment. After damaging the target equipment, the attacker next advertises their ability or skill in solving that particular problem. Thus, allowing the attacker to gain the trust of the target along with access to the targets sensitive information. If the attacker is successful; the target will continue to confide in the attacker for help in the future.

Categories of Social Engineering Social engineering attempts are classified under two categories of deception.

The categories of deception are identified as “ Technology-based” and “ Non-Technology based”. Technology-based social engineering is used to deceive computer users into believing that he or she is interacting with real applications or systems to get them to provide confidential information. Common examples of Technology-based social engineering methods include Pop Windows, Spam Mails, and Phishing. What is a phishing? Phishing is a form of social engineering that uses email and or malicious websites to steal personal information. Phishing attackers create emails and imposter websites that mimic legitament companies and organizations.

For instance an attacker may send an email posing as a reputable banking institution asking the victim to click on the provide web link to update their personal account information, thus allowing the attacker captures the updated information. Spam Mail Spam mails are E-mails that are sent with the intent to plant malicious code into the recipient’s computer or network. Spam mails appear to be E-mails that provide useful information by offering friendships, gifts, and or free pictures. The Spam mail entices the recipient to open the emails and attachments, which releases Trojans, Virus, and worms into the computers network.

Popup Window Popup windows are generated from a hackers rogue program. The popup will generate a message stating your application connectivity has dropped due to network issues. The Popup window will also request the user to enter his user id and or password to reconnect the application. The user would then enter his or user id and password to reconnect the system. The user later realizes that his system has been attacked without realizing his was the one to open the gate by provided his user id and password to the attacker. Acting as a Technical Expect

Acting as a Technical Expert is the most common Non-Technical Social Engineering Attack. This attack occurs with an intruder pretending to be a support technician working on a Network problem while requesting the user to let him access the workstation to fix the problem. Once the user provides the intruder access to the computer system the intruder can access and breach the network, leaving the network vulnerable to the intruder attack. Social Engineering Defense The Human element involved in Social Engineering attacks, makes Social Engineering attacks one of the hardest threats to defend against.

Although it is difficult to defend against; organizations and individual must implement safeguards to protect themselves from social engineering attacks. The safe guard should include a Documented Security policy. The policy should document terms and statements, which include Acceptable usage policy, Personal Security, Physical security, and Virus protection. 1. Acceptable usage policy -rules applied to restrict the ways the network site or system may be used. 2. Personal Security- Screening employees and or network users 3.

Physical Security- Securing the physical location of the networks devices from unauthorized access. 4. Virus protection- securing the network and it information from Trojans and virus treats Impact of Social Engineering A successful social engineering attack can be detrimental to an organization and or individual. The financial lost due to an attack can be punitive to an organization and its individuals. The attack can also disrupt or ruin an organization reputation. For example, an attacker could get access to the stored personal data of the organization vender or customer.

Once the vendor or customer becomes aware that their personal information has been breached they may no longer want to do business with the orgianization. This could lead to lawsuits against the company which lowers the organization reputation in the public eye. Loss of reputation can lead to loss of clients, vendors, and prospective business partnerships. The attack could lead to the overall failure of the organization. Conclusion Understanding the potential security threats, organizations must address social engineering threats as part of their overall security strategy.

The best way to mitigate the risk posed by rapidly evolving social-engineering methods is through an organizational commitment to a security-aware culture (Cisco 2011). Organizations and their IT departments must implement security awareness and trainings to ensure all personal can understand and recognize security issues and threats when they arise. Frequent IT security courses and or trainings can provide an organization and its personal the tools they need to recognize and respond to social-engineering threats, thus setting a presence of accountability that encourages active participation in the security awareness.

Works Cited Bakhshi, T. , Papadaki, M. , & Furnell, S. (2009). Social engineering: Assessing vulnerabilities in practice. Information Management &

Computer Security, 17(1), 53-53-63. doi: 10. 1108/09685220910944768 Cisco Systems Inc. (2011), Protect Against Social Engineering. Retrieved from http://www. cisco. com/web/about/security/intelligence/mysdn-social-engineering. html Granger, Sarah (2001), Social Engineering Fundamentals, Part I: Hacker Tactics. Retrieved from http://www. symantec. om/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics Mitnick, K. and Simon, W. (2002), The Art of Deception: Controlling the Human Element of Security, Wiley, Indianapolis, IN Peltier, T. R. (2006). Social engineering: Concepts and solutions. EDPACS, 33(8), 1-1-13. Retrieved from http://search. proquest. com/docview/234907988? accountid= 44759 Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Security Journal, 16(6), 315-315-331.