Chapter 6.3
Guarding Corporate Data from Social Engineering Attacks

Christopher M. Botelho
Baylor Health, USA

Joseph A. Cazier
Appalachian State University, USA

ABSTRACT

The threat of social engineering attacks is prevalent in today's society. Even with the pervasiveness of mass media's coverage of hackers and security intrusions, the general population is not aware of the possible damage that could occur should they be subjected to a social engineering attack. In order to show the damage caused by these attacks, we will discuss the results of a social engineering attack based on a survey conducted in the downtown area of a large financial center in the United States. The authors make suggestions companies can incorporate into their policies in order to protect their employees, as well as systems from intrusions based on social engineering attacks.

INTRODUCTION

As more and more organizations invest in technology to ease the delivery and dissemination of information, more opportunities are created for security incidents. Before the Internet was a part of everyday life, intruders usually gained access to sensitive data by physically setting foot on a company's premises and breaking into a safe or file cabinet. As a result, companies installed security cameras, door locks, and alarm systems.

Today, corporations still have these devices but must also protect their digital data. Investments in devices, such as intrusion detection/prevention systems to alert them of a security incident; firewalls to protect their internal network; and virtual private networks to ensure individuals connecting from the outside are authorized and have a secure connection are necessary expenses.

Another tool corporations use are organizational controls. These are processes and procedures put in place to control and protect assets, which include physical goods, buildings, money, and even a firm's reputation and image. Of the many types of controls, one of the most fundamental is access control. Access controls restrict access to your business systems to authorized personnel. These controls are key to information security and are one of the ten required

DOI: 10.4018/978-1-59904-855-0.ch037

domains of study for the certified information systems security professional (CISSP) certification exam (Krutz & Vines, 2001).

One of the most critical types of access control in today's internet-connected world is the use of passwords. We use passwords to access many of our online and company accounts (Zivran & Haga, 1999). Usernames and passwords are the most common form of authentication, but are also the weakest due to human error (Ciampa, 2005). One weakness of passwords is they are difficult to remember, leading people to choose weak passwords they can remember (Cazier & Medlin, 2006) and the tendency of people to reuse their passwords for multiple accounts, making the danger of a weak password greater as it can compromise multiple systems (Ives, Walsh, & Schneider, 2004).

Today, most network and system security devices rely on the username and password to grant access. As such, obtaining this information is the equivalent of hitting the jackpot for a hacker. When a hacker is attempting to break into a system, they want to find the quickest and easiest point of entry. The longer it takes to break into a system, the more information the hacker leaves to get caught in the end. Better security technologies are continually being invented to make it more difficult for an attacker to gain access. As a result, many hackers will rely on social engineering methods, that is, using social skills to obtain information, such as a user's password (Krutz & Vines, 2001), to gain access to a target since in many cases it is a lot easier to exploit a human than a system (Mitnick, 2002). The social engineer utilizes an arsenal of methods, allowing him or her to leverage the emotions of a victim, aiding in an attack. The social engineer can flirt with the victim in an attempt to gain information; make the victim feel guilty so they divulge information they would not have otherwise; or even convince the victim that their job could depend on giving the attacker the requested information (Mitnick, 2002).

With this research, empirical data is presented on the current susceptibility of social engineering attacks on companies. From this information, several suggestions are made for companies to ensure social engineers do not succeed. Recommendations are aimed at preventing potential attacks. Lastly, possible future research aimed at studying social engineering further in different areas is discussed.

BACKGROUND

Each day, numerous employees have access to sensitive data in order to do their job. Generally, they will use a password to access this data. Their password is one of the only things keeping a potential intruder out of their employer's network. In the event their password is compromised, the entire company's infrastructure is at risk. Social engineers use human weaknesses, such as trust and fear, to their advantage to exploit these people and get as much information as possible. With experienced social engineers, the employee will not even know what has happened and will continue their day without so much as a second thought. This creates even more risk, as not only does the social engineer have the employee's password, but he or she also avoids detection and possibly can have free roam of the company's network and systems.

Social engineering is the act of gaining either unauthorized access to a system or sensitive information, such as passwords, through the use of trust and relationship building with those who have access to such information (Damie, 2002). A social engineer uses human psychology to exploit people for his or her own use.

According to Kevin Mitnick, a prominent social engineer, "Savvy technologists have painstakingly developed information-security solutions to minimize the risks connected with the use of computers, yet left unaddressed the most significant vulnerability, the human factor"