Social Engineering Awareness

Security is everyone's responsibility

By Sean Colicchio, CISSP, CEH

April 2013

White Paper

essextec
GETTING IT DONE TOGETHER

INTRODUCTION

One morning, about a year ago, a stranger walked into a credit union with a letter typed from their home office. Using this letter, this individual was able to obtain access to the internal financial systems behind the teller counter - with permission and without supervision.

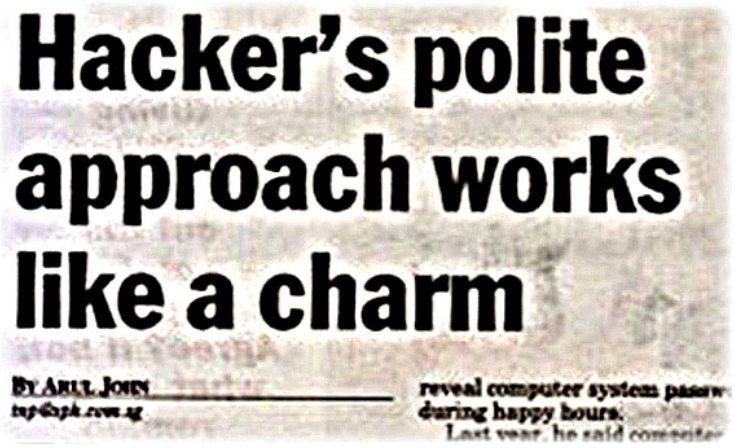
How did they do it? By obtaining small amounts of access - bit by bit from a number of different employees in that organization. First, they did research about the company for several days before even attempting to set foot on the premises. For example, they learned key employee's names by calling the Human Resources Department and researching various web sites. Next, they uncovered the type of software that the credit union used. Then they created a letter of permission on mock company letterhead that stated they were there to test the software. A friendly employee notified the manager and the manager opened the door for them.

SOCIAL ENGINEERING TECHNIQUES

Social engineering techniques are used in an attempt to obtain knowledge regarding perimeter network devices and their defenses (IP address ranges, firewalls, and default gateways) as well as potential internal targets. The purpose of this testing is to assess the ease of extraction of critical information from internal organization resources and employees/contractors or others with detailed knowledge of the organization, without their becoming aware of the importance of the information acquired. Of particular interest is testing whether the organization's staff will assist an unauthorized or unidentified user. The stranger knew the managers' names and branch locations, so they were able to enter each location with intelligence and obtain financial data off of the credit union computers. They dug through the corporate trash and found all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. From there, they used regular technical hacking tools to gain super user access into the system.

In this case, the stranger was a risk consultant performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO, but were able to obtain all the access they wanted through social engineering.

A friendly employee notified the manager and the manager opened the door for them.


Hacker's polite approach works like a charm

BY ARUL JOHN

reveal computer system passw
during happy hours.

BASIC GOALS OF SOCIAL ENGINEERING

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include: telephone companies, answering services, big name businesses, financial institutions, and hospitals.

Finding good, real life examples of social engineering attacks is difficult. Target organizations either do not want to admit they have been victimized (after all, to admit a fundamental security breach is not only embarrassing, it may be damaging to the organization's reputation) and /or the attack was not well documented so that no one is really sure whether or not there was a social engineering attack.

Social engineering attacks take place on two levels: physical and psychological. Regardless of the method used, the main objective is always to convince the person who is disclosing the information that the social engineer is a person they can trust with sensitive information.

The physical and psychological aspects of social engineering utilized impersonation, ingratiation, conformity, diffusion of responsibility, and trust in order to persuade the target. A formalized training program should be put in place in an organization in order to prevent these type of attacks. Everyone is responsible for organizational security - from the receptionist to the CEO and, unless employees are aware of this responsibility, the ability to mitigate security risks is severely impacted.

CONCLUSION

The truth is that the only way to prevent a successful social engineering attack is training and education. The human element of security is the weakest link in the security chain. As long as an organization's staff is educated, businesses will be fortified and defensive against attacks.

Everyone is responsible for organizational security - from the receptionist to the CEO.

> Dynamic Infrastructure > Data Management / Analytics > Business Risk Services

Essex Technology Group, Inc.
> 201 West Passaic Street
Suite 303
Rochelle Park, NJ 07662
> exceed@essextec.com
> 1-888-519-1518
> essextec.com

essextec
GETTING IT DONE TOGETHER