

Control Essentials

Volume II, Issue IV

April 2007

Business Consulting

- *Regulatory Support*
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- *Enterprise Support*
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- *Application Security*
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- *Network Security*
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

Social Engineering: Attacking The Weakest Link

Organizations invest unfortunate amounts of time and money trying to protect their networks from the continuous attacks of hackers. By keeping up with the joneses they are able to boast of technological upgrades, security and high-end encryption that ultimately benefit them in the long run. There is, however, one popular means of gaining access that bypasses technologies and technical systems completely. Welcome to the world of social engineering.

Security is only as strong as its weakest link. Social engineers attack the weakest link in a business process - people. Technology alone is almost helpless when this link is exploited, and this makes social engineering attacks one of the most dangerous attacks for an organization.

So how does one deal with social engineering? You would be wasting your time if you went around looking for a technical all-in-one solution. Mitigating social engineering attacks requires time and a series of efforts driven by policies and procedures that are reinforced, on an on-going basis, by security awareness and training programs.



Who are social engineers?

Social engineers are talented and smooth individuals who exploit human vulnerabilities, such as ignorance, naiveté and the natural desire to be liked by or be helpful to others. Social engineers, in essence, "hack" humans to obtain useful information that allows them to gain access to the assets of an organization. Answering the question "What assets in my organization are potential targets?" is a good starting point to counter social engineering.

How do they attack an organization?

A social engineer often pretends to be a character, such as a technician, a customer, a vendor/client representative, etc., to deceive an organization's employees. Social engineers are well known to have a score of tricks up their sleeve such as mentioning the name of an executive or other employees and/or using appropriate terminology to build credibility or if nothing works, just plain smooth-talk. Establishing credibility is essential for an attack to succeed.

An attacker could introduce himself as someone offering to help the victim solve a problem that he/she caused. In addition, an attacker may also try to convince the victim that they share common interests, hobbies or goals. The attacker could also pretend to require immediate help from the victim. Other productive strategies include the use of fear to scare employees (junior staff is particularly subject to this strategy) to obtain the desired information. For instance, the attacker could pretend to be a senior manager who requires critical information. It is likely that employees will provide the attacker with the information without any challenges to avoid unpleasant confrontations.

Design your defense

Policies and Procedures

Security policies aimed at mitigating social engineering attacks should provide guidelines on employee behavior in order to properly protect information and reduce the probability of a successful attack. Policies and procedures should be written in a manner that can be easily understood even by non-technical employees.



Policies and procedures often fail due to lack of clarity. It must be ensured that the policies and procedures are documented in a lucid manner, clearly emphasizing why each policy is important. This will gain employee buy-in, which is paramount for the success of any security policy. Further, employees should also be made well aware of the consequences for failing to comply with security policies and procedures. At the same time employees who demonstrate dedicated adherence to security practices should be publicly rewarded.

Implementing a security policy is a gradual process that requires time and perseverance. Security policies often require people to change their habits to conform to security requirements. Without the cooperation of all employees, policies become ineffective. Hence, there is a definite need for on-going awareness and training programs. These programs instill the appropriate behavior and attitudes that should be recognized by employees. Moreover, the existence of the program will only motivate them further to comply consistently with the policies.

Security Awareness and Training Programs

Organizations are composed of various departments. It is essential that training and awareness programs should be customized to meet the requirements and needs of the target audience. Active support of senior management should be visibly incorporated into these programs.

Awareness programs have the primary scope of keeping employees up to date with the topic of social engineering attacks. The program should adapt humor and creativity to keep employees interested. Several inexpensive mediums such as newsletters, brochures, posters, coffee mugs, mouse pads, screensavers, etc. can be used effectively in a security awareness program.

Security awareness and training programs should be mandatory. Particular attention should be given to new employees and those employees being promoted as their training needs to be tailored according to the responsibilities related to the new position. Effective training sessions have been known to use role-playing to demonstrate personal vulnerabilities to social engineering attacks.

Summing it up

Social engineering is a very real threat and one that currently has a fairly free reign. The security of an organization is rooted in its security policy and practices. However, employees can make or break organizational security as they are the implementers.

Building a "security culture" in an organization is the first step to minimizing an organization's risk of falling prey to social engineering attacks. Security policies, training and awareness programs serve as the fundamental tools to promote such a culture. The need today is to ensure that the people of an organization are made "hackproof".



Their consultants are more seasoned than typical *Big 4* firms.



Known technical quality at less than *Big 4* firm rates.

We selected ERM because of their professional references, experience and reasonable professional fees.



ERM accomplished and exceeded objectives planned.

We accomplished our objective of a high-quality service within the budget stipulated for the project.



Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

We encourage you to visit our website, www.emrisk.com, for details on ERM's services, team profile, clientele and testimonials from some of our clients.

For further information, please contact an ERM consultant at (305) 447-6750.