SOCIAL ENGINEERING |
TEST YOUR NETWORK BEFORE SOMEONE ELSE DOES

DataComm

You are busy at work and you just finished a meeting with a coworker. You receive a call letting you know there's a technician at the front desk. When you greet the technician, he shows proper identification and explains that he's there for some routine maintenance. You bring him to the network closet, but something requires your immediate attention. Before you know it, your network has been penetrated and countless assets have been compromised.

The term "social engineering" has been used for years by hackers to describe the technique of using persuasion and/or deception to gain access to information systems. Such persuasion and deception is typically implemented through human conversation or other interaction. Institutions throughout the United States have contracted with DataComm to test their existing security policies and procedures and to recommend new ones. During these tests, our certified security engineers use varying attack schemes to gain unauthorized access and to obtain critical confidential information. Three common attack schemes we have identified include:

- Phone calls to individuals within the organization. This will normally include the helpdesk and specific individuals that are identified as critical company personnel.
- Carefully crafted phishing emails combined with website spoofing that is targeted to specific groups or individuals in an attempt to coax information from the recipient.
- A thumb drive or CD with an enticing label such as "payroll" or "confidential" that is left in a hallway, breakroom or restroom in specifically targeted locations. On the media will be malicious code.

Comprehensive reporting and follow-up staff training are available to help you resolve areas of weakness. Your security is only as strong as the least prepared employee in your organization. The strongest of network security appliance can be bypassed by uncovering a weakness in a single employee. Make sure your security extends to all parts of your organization.

3 KEY INGREDIENTS

- **Comprehensive Event Collection** - Collects application, system, & security event data on critical devices.
- **Real-time Alerting & Notification** - Alerting allows you to set the specific criteria on hosts for which you need to be notified.
- **Compliance Logging & Reporting** - Generate predefined reports to meet HIPAA, GLBA and SarbanesOxley requirements.

DID YOU KNOW?

The average cost of an attack originating from outside an organization is $57,000, while the average cost of damage incurred from an internal attack is an astounding $2.7 million.

- CSI/FBI Computer Crime and Security Survey

SOCIAL ENGINEERING |
TEST YOUR NETWORK BEFORE SOMEONE ELSE DOES

DataComm

HOW IT WORKS

DataComm offers an extensive social engineering program that can be conducted on-site and remotely:

- **On-site Social Engineering**
  On-site assessments include attempts to gain physical access to the premises, obtain records, files, equipment, information, network access, and more. All tests are conducted in a very strict and professional manner.

- **Remote Social Engineering**
  Remote testing includes a wide range of attacks designed to compromise your policy and access confidential information and provides important information on how your staff will respond to potential security threats.

- **Security Awareness**
  Many institutions want to perform an assessment of their employee's compliance with the current information security policies and procedures. The need for social engineering has never been more in demand than now.

- **Locate the Problem**
  DataComm's social engineering can root out and document potential areas of weakness. We will identify areas that need improvement, document compliance shortfalls pertinent to regulatory agencies, and assist you in developing security awareness training to fix the issue.

Our methodology mirrors our approach to security assessments. We begin with target identification and information gathering, followed by exploitation attempts. We systematically apply these principles in a customized approach which depends on the objectives of the particular situation. We work closely with our client to define the test scenarios. The test scenarios are tailored to test-specific policies and processes within their organization. Some organizations may have incident response procedures in place to report suspicious phone calls. DataComm can test these procedures by making obvious attempts at gaining confidential information without proper authorization. This is an excellent way to test the effectiveness of a security awareness training program, or lay the foundation for creating an awareness program.

COMPREHENSIVE REPORTING

Reports are only as good as the products and people that produce them. Our elite team of security experts is comprised of senior security professionals who have honed their skills through corporate security leadership, security consulting, investigative branches of the government, research and development. Comprehensive reporting and follow-up staff training are available to help resolve areas of weakness and help employees better understand corporate policy and the risks that may exist.

A COMMON MISCONCEPTION

Most people think computer break-ins are purely technical, the result of technical flaws in computer systems that the intruders are able to exploit.

The truth is, however, that social ngineering often plays a big part in helping an attacker slip through the initial security barriers.

Lack of security awareness or gullibility of computer users often provides an easy stepping stone into the protected system in cases when the attacker has no authorized access to the system at all.