

MITNICK SECURITY CONSULTING, LLC

SERVICES OVERVIEW

WINTER, 2004-2005

MITNICK SECURITY CONSULTING, LLC

7113 WEST GOWAN ROAD
LAS VEGAS, NV 89129
(702) 940-9881 TEL (702) 548-6505 FAX

MITNICKSECURITY.COM

SERVICES OVERVIEW

DATA SECURITY

MITNICK SECURITY CONSULTING, LLC

Mitnick Security Consulting, LLC is a full-service information security consulting firm. Founded by Kevin Mitnick, Mitnick Security Consulting offers a comprehensive range of services to help businesses protect their valuable assets.

Information security is essential in order to prevent potentially costly and embarrassing security lapses. Mitnick Security Consulting provides detailed assessments of their clients' entire security infrastructures to identify and ameliorate any vulnerability. As an early pioneer in the world of hacking, Kevin Mitnick has more than twenty years of experience identifying and exploiting weaknesses in information security systems among some of the world's largest corporations. Mr. Mitnick and Mitnick Security Consulting bring their unique experience and the latest technology to address their clients' vital security needs.

Mitnick Security Consulting works closely with its clients to address each client's security concerns without disrupting their ability to do business. Mitnick Security Consulting's services are not limited merely to identifying and recommending effective countermeasures such as patching existing security vulnerabilities. Rather, the company is dedicated to helping its clients develop and maintain an integrated security infrastructure that can prevent and minimize the effect of future security lapses.

Following its vulnerability assessment, Mitnick Security Consulting delivers a detailed written report to its clients advising them what systems were tested, which techniques were used, the public or proprietary tools and applications used in the "attack", what vulnerabilities were detected, and recommendations for improving security.

Mitnick Security Consulting provides a wide range of security assessment and testing services, including the following:

INTERNET SECURITY TESTING

Any device with access to the Internet is a potential open door to would-be hackers. Mitnick Security Consulting provides vulnerability assessments during which it closely maps the network architecture, examines all open ports, hosts and services with access to the Web, and ensures that these network devices are secure. Defensive thinking gathers information such as domain names, IP network ranges, operating system and applications, to identify systems on the network, how they are related, the services that are exposed through open ports (such as http, SMTP, terminal services, etc.). Once open ports and attached services are identified, Mitnick Security Consulting determines whether each service has been updated with the

most recent patches and identifies other vulnerabilities located within the exposed services.

In addition to conducting vulnerability assessments, Mitnick Security Consulting performs more rigorous penetration tests in which the information gathered from its assessment is used to attempt to penetrate the network. This more thorough procedure can confirm whether potential vulnerabilities are, in fact, capable of being exploited to expose the network.

Following all vulnerability assessments and penetration tests, Mitnick Security Consulting uses the information it gathers to prepare a thorough vulnerability analysis and offers recommendations for strengthening network security.

INTRANET SECURITY TESTING

While outside threats must be guarded against, business must also protect against potential threats from within their own networks. Using many of the same techniques and procedures for Internet Security Testing, Mitnick Security Consulting provides Intranet risk assessment and analysis to protect against the potential threat posed by insiders.

Depending on the client's needs, intranet testing can be performed by Mitnick Security Consulting under varying degrees of disclosure of network information from the client, for example with or without network accounts.

DIAL-IN RAS SECURITY TESTING

Dial-in links pose a potential threat to the integrity of the network security system. Mitnick Security Consulting examines dial-up connections that allow employees to access the network through public telephone lines or other dial-up connections. Given a range of telephone exchanges that may include modems, Mitnick Security Consulting can identify target numbers that allow for remote access. Using these numbers, Mitnick Security Consulting attempts to exploit vulnerabilities in the system and gain access to the network. Mitnick Security Consulting can also assess risks posed by the exposure of dial-up connections to the public telephone network which might undermine the client's own internal security architecture.

WEB APPLICATION ASSESSMENT

This assessment examines what services are being offered on Web-based portals and e-commerce applications to examine potential vulnerabilities with respect to authentication, authorization, data integrity, data confidentiality, and consumer privacy concerns. Mitnick Security Consulting can test these applications using either zero-knowledge testing or full-access testing to examine the full range of potential vulnerabilities. Mitnick Security Consulting also conducts source code audits to identify any potential vulnerability among the applications and scripts that are accessible through the Web.

WIRELESS ASSESSMENT

Wireless networks, while highly convenient, present additional security threats since the wireless signals are not limited by the physical boundaries of a traditional network. Mitnick Security Consulting evaluates how to prevent wireless communications from being exposed to eavesdropping and access by unauthorized intruders. Additionally, Mitnick Security Consulting examines the enterprise infrastructure for unencrypted or standard WEP enabled access points that may be vulnerable in order to ensure the security of the network.

SOCIAL ENGINEERING ASSESSMENTS

Social engineering involves manipulating and/or deceiving company employees and other human resources to gain unauthorized access to a network or to confidential information. Mitnick Security Consulting is the premier consulting firm in its ability to identify weak links in the security chain through exploitation of human vulnerabilities.

Mitnick Security Consulting's principal, Kevin Mitnick, is widely recognized in the industry as the foremost authority on the topic of social engineering. His book *The Art of Deception: Controlling the Human Element of Security* offers an authoritative examination of potential threats posed by social engineering attacks. Mitnick Security Consulting leverages its unparalleled expertise in this field to expose what is often the weakest link in the information security apparatus: the human element.

Once individual or systemic weaknesses are identified, Mitnick Security Consulting recommends procedures designed to ensure that employees do not divulge information that could compromise company assets. The social engineering assessment not only uses tactics intended to gain confidential information, but also to induce unsuspecting employees to create vulnerabilities that can subsequently be exploited to gain access to confidential information.

TELECOMMUNICATIONS ASSESSMENT

Mitnick Security Consulting has unique experience testing vulnerabilities in private bank exchanges that operate company voicemail and messaging systems. Unauthorized access to these systems can allow an intruder to eavesdrop on and manipulate employee voicemail messages, initiate outgoing calls from internal company lines, and access corporate telephone networks and directories.

DATABASE ASSESSMENT

Client lists, credit card records, and other confidential information held in databases must be given particular protection from unauthorized disclosure. Mitnick Security Consulting tests database integrity to determine whether any vulnerability may compromise this sensitive information.

PHYSICAL SECURITY TESTING

Access to confidential information can often be obtained by simply gaining physical access to company premises. Mitnick Security Consulting conducts on-site surveillance to assess physical security and uses social engineering, pass key duplication, and other techniques designed to gain physical entry into secure areas and the network system.

FORENSICS

In addition to preventing future attacks, Mitnick Security Consulting can conduct forensic analysis to evaluate past security breaches. This analysis examines log reports, compares backups to identify modifications to the network, and investigates the introduction of foreign software tools to help identify intruders, determine the extent to which the network has been compromised, and mitigate potential damages from the intrusion.

TRAINING

Mitnick Security Consulting provides training seminars to IT professionals and employees with access to sensitive information to better educate them about the risks of social engineering and how to prevent themselves from falling prey to ruses posed by competitors or malicious intruders. These seminars are dedicated to preventing human error from undermining an otherwise robust information security infrastructure.

For more information on your needs, please contact us directly at:

MITNICK SECURITY CONSULTING, LLC

7113 WEST GOWAN ROAD
LAS VEGAS, NV 89129
(702) 940-9881 TEL (702) 548-6505 FAX

MITNICKSECURITY.COM