CASE STUDY

HITACHI
Inspire the Next

PENETRATION TESTING FOR THE TELECOMMUNICATIONS INDUSTRY

Hitachi Systems Security Inc.'s technical security audits will provide you with the answers and recommendations you need to improve your security posture and protect your organization's most valuable assets. Technical security audits detect the vulnerabilities that can be used by unauthorized users and uncover the weaknesses of your organization's security processes. They are carried by our certified security consultants (ethical hackers) who simulate attacks by using the same techniques as a malicious attacker. The objective of such an audit is to evaluate if your organization's informational structure can be easily accessed without authorization or not.

QUICK FACTS

Industry: Telecommunications

Needs & Requirements:

- Improve security posture to better protect corporate IT assets against vulnerabilities and intrusions
- Identify and implement remediation measures for corporate vulnerabilities
- Report findings to executive team

THE CHALLENGE

The telco's Information Security Manager was under a lot of pressure and faced with a huge challenge – providing the executive board with an overview of the telco's security posture and implement effective solutions to improve it, all while staying within a strict limited budget. The telco's Vice President of Information Systems shared the following concerns:

"Could cyber criminals access our customers' personal data?"

"Are our internal information systems secure enough that even an ill-intentioned employee could not access confidential information?"

THE SOLUTION

- To identify the most critical information assets and to perform tests on a representative sample of the external and internal information infrastructure.
- To simulate automated and manual attacks in order to determine the permeability of the information systems.

DELIVERABLES

The final result of the penetration test was a detailed report that included all the findings of the test as well as the countermeasures and recommendations to secure the customer's IT infrastructure. The report documented the following elements:

- The security level of the servers as perceived by an attacker.
- The security breaches, vulnerabilities, as well as countermeasures and corrective actions to be applied.
- All testing activities and raw scan data are also provided alongside the final deliverable as report appendixes and supporting documents.

All serious vulnerabilities that were discovered in the course of this evaluation were sent to the customer as an interim report.

MAIN BENEFITS

- Obtain a clear vision, for the executive board, of the existing information risks
- Improve information risk management by knowing those risks
- Limited costs associated to tests (technical audits)
- Higher protection of the subscribers' confidential data
- Proper management of the internal access privileges
- Improve protection against technological weaknesses that can lead to intrusions, frauds and service interruptions

SERVICES PROVIDED

A team of Hitachi Systems Security Inc.'s Senior Cyber Security Experts collaborated on this engagement:

Internal Intrusion Test
The internal infrastructure was tested in “grey box” mode, meaning this company created an employee account with limited access privileges for Hitachi Systems Security Inc.'s consultant. Our consultant's mandate was to try to obtain access information that an employee would normally not have access to.

External Intrusion Test
The security assessment of the Internet website and of the external network was performed by deploying an optimal mix of automatized tools and “ethical hacking” techniques, mastered by our consultants.

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada
Tel: +1 450-430-8166   Fax: +1 450-430-1858
www.hitachi-systems-security.com