

Case Study – Attack Tree Methodology

Our passion for technical excellence and commitment to our clients' business success results in practical solutions to complex problems.

Contact Us:

Network & Security
Technologies
161 North Middletown Road
Pearl River, NY 10965

Phone:
(845) 620-9500

Fax:
(845) 512-2093

E-mail:
info@netsectech.com

URL:
www.netsectech.com

Subject Area/Specific Service:

Comprehensive Security Review for large US based electrical utility of their electrical substation infrastructure.

Date of engagement:

Q2-Q3 2008

Brief description:

One of the largest energy utilities in the US has operations affecting regions of the country. The client required a dynamic enterprise view of their security risk as well as a prioritized remediation plan aimed at protecting their business operations. In a world defined by limited budgets, resources and time in the context of many vulnerabilities, attack points and attackers, N&ST needed to build a risk assessment methodology that would economically address these requirements across a large number of locations and technologies.

N&ST Recommended Solution(s):

Considering the complex and varied environment, N&ST realized that it needed to pull together an innovative approach in order to provide real value to our client on an enterprise basis. N&ST used an Attack Tree Analysis methodology to provide a framework for this firm to understand the varied risks and consequences of these risks. By mapping out the sets of attack and sub-attack scenarios, as well as the possible threat actors, N&ST was able to help our client take action on priorities and make well-reasoned decisions. Human behavior is also incorporated into our modeling by using indicators to profile specific attacker's behavior.

Client actions:

Client has been able to prioritize remediation efforts as well as institute protective measures to reduce the consequences of any modeled attack scenario.

Problems remaining:

Client realizes that this framework is vital for their complex and varied environment. N&ST continues to work with Client to build a library of modular attack paths.

Lessons learned:

Complex problems require experienced teams. If we had pursued the "traditional" approach to security assessment, N&ST would have exhausted the client's budget without really providing any broad value or strategic direction.

Client Comments:

"N&ST provides a 'unique and different type of security consulting' than commonly seen from other security firms. They have a knack for making complicated things simple."