Does Your Connection to the Internet Keep You Awake at Night?

Introduction
More than ever before, companies are relying on the Internet to assist them with their day-to-day business activities. As more and more employees require access to the Internet, firms are implementing high speed connections to the World Wide Web. Companies realize there are security risks in connecting their IT systems to the Internet and are installing firewalls to protect them from potential intruders. The firewalls are a first step in securing their systems, but are only a part of a total security solution. This article identifies various risks and how leading organizations are using risk assessments to help them protect proprietary and sensitive information while getting more out of their existing IT investments.

Background
Most organizations have a need for employees to access data from remote locations. How can an organization identify legitimate traffic from an intruder masquerading as a company employee?

One of the first steps in protecting your equipment from an Internet intruder is the installation of a firewall. The firewall is placed between your high speed connection to the Internet and your in-house equipment. Most firewall systems are able to monitor traffic coming in from and going out to the Internet. With special “rules”, the firewall can be configured to block intruders from accessing your equipment. These same “rules” may allow a company to restrict certain employees from accessing the Internet.

A company must examine many factors in order to arrive at the best possible solution for connection to the Internet. An alternative that may work for one company may not be feasible for another. Some organizations are using Virtual Private Network (VPN) technology to allow remote connectivity to corporate data. Unfortunately, VPN technology by itself is not sufficient. If the remote user does not have his system adequately patched, an intruder may gain access to that device and then piggyback on communications to the corporate office.

Firewall Considerations
Basic firewall considerations during the design, implementing and overseeing process include:

- Objectives. Determining the overall objectives of the firewall. In this initial stage, the acceptable level of risk and operation of the firewall are considered. Should the firewall deny all access except those critical to the mission of connecting to the Internet? Should it provide an audited record of activity?

- Needs analysis. Establishing a checklist through a needs analysis and risk assessment. Once the level of risk has been determined, a company must decide what needs to be monitored, permitted and denied.
- Financial. Implementing solutions according to financial considerations. Lower end solutions may include routers, Microsoft Proxy Server or "solutions in a box". Higher end implementations may be required in order to protect your in-house equipment from Internet intruders.

Companies must determine which firewall solution is best for their specific needs. Using the resources of a firm that specializes in firewall solutions provides additional assurance that the company will achieve its goals and objectives. Some considerations:

- Firewall Limitations. Firewalls have limitations and can't protect companies from all types of attacks. Discover the top 10 firewall limitations and their impact to your organization.
- Eliminating Single Points Of Failures (SPOFs). Most companies know that a firewall is only part of a total security solution. Short of having a hacker try to breach your security, a company may not be sure how protected they really are. Fortunately, security solutions are available to analyze a company's potential for risk.

Network security audits evaluate your security controls to determine your exposure to intruders. Such professionals typically run assessment software that analyzes your equipment and pinpoints areas of concern. Your organization then has the option of making the necessary appropriate adjustments yourself or relying on the assistance of outside technical personnel. After the necessary corrections have been made, the security professionals examine the company's equipment a second time to verify the accuracy of the work that was performed.

Summary

High speed connectivity to the Internet increases employee productivity while increasing risk from outside intruders. Firewalls are a first step, but are only part of a company wide security solution. Network security audits identify, manage, and reduce risks and give an organization a competitive advantage in its marketplace.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.