Key Considerations for Outsourcing Security


Introduction

As last summer’s virus attacks vividly demonstrated, companies of every size are finding themselves hard pressed to maintain around-the-clock network security. Arriving nearly simultaneously, the Blaster, Welchia, and Sobig.F worms invaded hundreds of thousands of corporate computers, resulting in billions of dollars of damages and lost productivity. In this new atmosphere, where crippling attacks arrive almost immediately after vulnerabilities are announced, how can enterprises maximize their IT investments and successfully manage security? They can tackle the job with their in-house IT staff, of course, or they can outsource the task to a managed security services provider (MSSP). This article will look at certain key issues for determining when outsourcing security is the best approach to take.

Scrambling to find the resources

One thing the viruses mentioned above made clear is that the changing nature of cyber attacks has turned security into something of a moving target for enterprise operations. Constantly evolving threats relentlessly expose gaps in these companies’ security systems. And that has produced a singular dilemma.

According to research and advisory firm Gartner Inc., at most companies, the staff responsible for IT security functions is also responsible for other activities and spends most of its time on non-security projects. For any resource-constrained organization, the added responsibility of managing security is often just too taxing. Gartner has concluded that in-house teams struggle to understand and defend against the latest security threats because this requires constant system monitoring – something that few businesses can afford.

For those IT staffs that take on the task, the challenges are daunting. After all, this normally entails formulating a security policy and implementing firewall, intrusion detection, virus detection, and other security technologies. But even after taking these steps, the challenge remains of how to manage the security effort. Security, after all, isn't static, and enterprises must be prepared to proactively monitor, maintain, and upgrade their network protection.

The bottom line: maintaining the necessary vigilance in these days of “zero-day” attacks requires significant investments in staff, IT systems, and training.

Selecting an MSSP

The alternative is for enterprises to outsource the management and monitoring of their network security to an MSSP. An MSSP can combine advanced technology with expert human analysis, enabling an enterprise to cost-effectively strengthen its security posture. An MSSP can also provide a level of technology and expertise that ensures rapid response to real threats.

Specifically, a capable MSSP must employ advanced data mining and security event correlation capabilities to enable it to accurately correlate, analyze, and interpret large volumes of network security data in real time. In general, an MSSP’s services include timely phone and email access to security monitoring staff and Web access to reports on such things as device status, change requests, and service level performance. Perhaps most importantly, these services enable enterprises to focus resources on their core, everyday business issues.

The stakes are certainly rising. In its recently issued predictions for 2004, Gartner said enterprises will choose service providers based not on the provider’s ability to recognize intrusions and alert the enterprise, but rather on its ability to recognize critical vulnerabilities and to block attempts to exploit these vulnerabilities. Gartner expects demand for managed security services to increase at a compound annual growth rate of nearly 31 percent through 2005, and predicts that all major managed security service providers must offer external and internal vulnerability scanning and threat assessment as integral components of their device management services if they are to be serious contenders in the MSSP market. (That will be particularly relevant given enterprises’ efforts to comply with auditor requirements stemming from legislation such as the Sarbanes-Oxley Act.)

The conclusion is unavoidable: any notion that security is a matter of simply protecting the network perimeter is hopelessly out of date. Why? Because increasingly, enterprises are recognizing the importance of “defense in depth.” This involves a comprehensive approach to securing critical assets, networks, and information systems while implementing robust defenses against hackers, viruses, and other online threats. Defense in depth recognizes that today’s environment is one increasingly beset by so-called blended threats that dynamically target the vulnerabilities of isolated security products. As a result, companies must adopt a deep, integrated strategy that addresses security at all tiers: gateway, server, and client. It is precisely this kind of strategy that an MSSP can help enterprises execute.

So how should an enterprise go about choosing an MSSP? The following criteria should be considered:

**Longevity.** Entrusting sensitive corporate data to a third party is not a decision to be taken lightly. When partnering with an MSSP, invest the time and resources to ensure that the service is addressing your organization’s most critical needs. As a result, special
emphasis must be placed on choosing a partner that has a proven track record of delivering quality security services to a broad range of industry sectors over a long period of time.

**Real-time analysis and response.** An MSSP must have the ability to accurately correlate, analyze, and interpret large volumes of network security in real time. It must be able to separate real security threats from a welter of “false positives.”

**State-of-the-art facilities.** An MSSP should have multiple security operations centers, or SOCs, that run 24x7x365. Having two or more SOCs allows for cross-monitoring, ensuring constant compliance with security standards. They can also provide backup in times of disaster.

**Global intelligence.** An MSSP should have security experts positioned to monitor and analyze data from customers around the world. This global intelligence enables an MSSP to issue real-time alerts and recommend actions to be taken in a timely fashion.

**Annual revenues.** What is the prospective MSSP’s financial status? For publicly traded companies, Gartner estimates that annual run rates of more than $10 million per year in managed security services contracts indicate a sufficient base of revenue to support growth and enhancement of services.

**Management experience.** For leading MSSPs, management experience will include backgrounds in military, government, and industrial sectors.

**Breadth of services.** This key consideration indicates an MSSP’s ability to meet the security management needs of a wide variety of companies. It includes real-time monitoring and management of firewalls, intrusion detection systems, virtual private networks, and other security products.

**Security management processes.** An MSSP should be able to provide documented standards and policies for handling typical and atypical operations and threats. An MSSP should offer a variety of attack alert notification methods to allow customers’ staff the ability to mitigate risk in real time.

**Vendor neutrality.** An MSSP should employ security specialists with certified expertise across a broad range of security products from a variety of security providers. This allows a company the freedom to select best-of-breed solutions.

**Auditing.** While trust is one of the most important factors in selecting an MSSP, the vendor must have facilities, processes, and procedures in place that are validated and certified by a third-party auditor.

**Reporting.** Reports provided by MSSPs should be detailed enough to support decisions to enhance security efforts and to determine the cost-effectiveness of the managed services. Thorough reports will include information gleaned from the managed devices, recommended responses, any changes the MSSP made to the devices, and information about the latest threats. In addition, enterprises are increasingly reacting to legislation (such as Sarbanes-Oxley) that will entail stringent compliance reviews. An MSSP should therefore be in a position to consolidate and analyze security log data.

All organizations can benefit from the continuous management and monitoring of their security operations. In this regard, an MSSP can help develop a company-wide security policy that sets appropriate access control rules governing all employees. This is essential because it recognizes that the majority of security breaches come from within. (Most MSSP contracts include monitoring of all security-related activities on the internal network.) Before signing on with an MSSP, make sure all employees are aware of the corporate security policy and what the MSSP is contracted to do.

**Conclusion**

Managed security services can remove the volatility associated with IT staffing and the need to respond to unpredictable network threats, allowing enterprises to better manage their day-to-day business requirements, resources, and costs. This is especially important today as threats increase in severity and complexity. Enterprises that are seriously considering outsourcing their security should know that this can be a smart business decision, as well as one that assists them as they face new reporting requirements.