Global Information Assurance Certification Paper

Managed Security Services - An Evolving Security Solution!

Babu Amaladoss
8 March 2001

Recent Distributed Denial of Service (DDoS) attacks or hacking on 'Yahoo!' 'World Economic Forum in Davos, Switzerland' and 'Microsoft' and virus/worm attacks such as 'I Love You', 'Koumikova', etc. have caused considerable damage and cost millions of dollars on big corporations. And this made them realize the importance of appropriately securing their information resources. But these companies do not have either adequate specialized security professionals or the time to attend to the constantly evolving security issues.

To make things even harder, the Internet and e-commerce are creating a rising demand for security. The new and demanding technologies, a rapid growth in remote access needs (PCS, handheld devices, etc.), rise in the streaming medias, complexity of networked devices and systems make managing security a full time task. Companies are increasingly opting to outsource their services related to the network security because of the in-house IT organizations' limited ability to perform the needed security management tasks to protect valuable assets from both accidental and intentional damage.

Many businesses hire security guards from another company for protecting their premises and banks hire another security company to drive their money around town. More and more firms are attracted to outsourcing all security services because an outsourced company can provide an aggregation of expertise and experience that it would be impossible to replicate in-house.

The traditional brick-and-mortar companies already have experience in the security lessons. However, dot-coms are under tremendous pressure to show profits early that they do not have time and the resources to attend to the security issues. That has opened up the market to Managed Security Service Providers increasingly.

Thus, Managed security services are projected to be one of the fastest-growing markets over the next several years. The 2001 Information Security Industry Buyers' Guide, published last month, lists more than 50 companies under the managed security services category. The Yankee Group, in preparing its managed security market forecast last month, tracked more than 80 such companies.

What Do MSSPs Offer?

Many firms with highly qualified professionals, who have expertise in network security, offer services to clients to manage the security of their organization's networks and information resources. Security requires resources, expertise and capital and these three things are tough for business users to fork over - especially the small and midsize enterprises.

These firms, or the Managed Security Service Providers as they are called, typically partner with certain vendors to provide integration and professional services to their customers. “Some providers offer pre-implementation managed services, such as penetration testing, vulnerability assessment scanning and Internet/perimeter security evaluations. Others implement technological solutions and services based on the initial assessments. Still others offer ongoing monitoring and management of products after their implementation”.

The following are some of the most common services offered by MSSP:

- ***Review of the current network services***
  Consists of analyzing the network topology, testing for vulnerabilities, reviewing the security policy.
- ***Installation***
  Install the hardware and software such as Firewall, etc. and provide support.
- ***Managed firewalls***
  Configure and manage the firewall installations.
- ***Data encryption***
  Helping companies to use high level data encryption for confidential e-mail and files that they need to protect from eavesdroppers.
- ***Anti-vandal and anti-viral filtering***
  Installing anti-virus software including regular updates and monitoring all suspicious network activities.
- ***Intrusion detection and response***
  Real time monitoring of intrusions and the appropriate response plan.
- ***VPN components***
  Configure and manage the VPN services for dialing into the company’s network.
- ***Total Security Solutions***
  A combination of all or some of the above mentioned services.
- ***Security administration and technical support***
  Auditing at regular intervals for any unusual activities on the network and providing a technical support that suits the client’s needs.

MSSP's are responsible to install and maintain the systems necessary to successfully stop security breaches and respond adequately to incidents. They provide and monitor their own proprietary security products, work with other companies to offer security as part of a total solution to clients' requirements. They now can perform real-time monitoring that could save a lot of precious time and money for the corporate customers and allow them to "focus on their core businesses".

Types of MSSPs

Managed security service providers (MSSPs) are all-in-one type of companies that come from different backgrounds. "They come in various forms: start-up companies, established computer security firms, large telecommunications and computer companies, Internet and application service providers (ISPs and ASPs), and consulting firms". These companies can be broadly classified as follows:

Established Network Companies: Many well-known network/security companies have entered the MSSP bandwagon. Since they already work in the related field this is only an extension to their existing services.

Some examples of this are:
The Salinas Group (http://www.salinasgroup.com/),
Counterpane Systems (http://www.counterpane.com/),
TruSecure Corp (http://www.trusecure.com/),
METASeS (http://www.metases.com/)

Original Equipment Manufacturers: Many security software manufacturers have launched managed services to complement their product offerings.

Few examples include:
Computer Associates (http://www.ca.com/),
Internet Security Systems (http://www.iss.net/),
Check Point Software Technologies (http://www.checkpoint.com/),
Symantec (http://www.symantec.com/)
Network Associates (http://www.nai.com/).

Joint Venture with ISPs/ASPs: Some Internet and application service providers partner with MSSPs or security product OEMs to offer security services. This actually is very attractive to the client as they get everything from one vendor.

Such providers include AT&T/ IBM Global Network, PSInet, Sprint, Earthlink and UUNET.

Suggestions For Selecting MSSP

It is rather very difficult to determine who would need a MSSP as every organization's needs, policies and the available skills would influence this decision. It is necessary to keep in mind that even outsourcing without proper verification could result in security breaches. It is absolutely necessary to do a thorough assessment of the MSSP before deciding to go outsourcing. Once the decision is made to outsource the security management, evaluation of MSSPs and their specific offerings can be initiated.

One of the things to look for in a good MSSP is variety. If a provider has partnerships with many vendors, this could be an indication that they are interested in providing the right solution. If a provider only offers one or two hardware and software platforms for their managed firewall solution, then they more than likely are an extension of the vendor.

The following are some good questions to be considered while selecting a MSSP:

- Do they assess the current network services?
- Will they assist in creating or refining a security policy?
- What services do they offer? Are these the latest versions and how often are these upgraded?
- Do they provide single product or a combination of products? Are there facilities for integrating new technologies?
- In the event of an attack, how soon will they respond? What is their support policy?
- What security vendors do they partner with?
- Will their security experts support the existing applications?
- How often do they monitor? Is it a real time monitoring? How do they respond to an incident?
- Do they perform vulnerability testing and what would be the frequency of these tests?
- Do they support different kinds of products or only their vendor's? Are they available for support on 24/7?
- Last but not the least, do the services cost more than the assets that need to be protected?

Further, these additional issues may be carefully checked.

Verify the MSSP's references and credentials thoroughly.

"The Service Level Agreement (SLA) may be the single most important part of any MSSP contract. The SLA is going to define the roles the client and the prospective MSSP are going to fill".

The SLA should be flexible to accommodate the constantly fluctuating Internet environment. Hence, the client and the MSSP should be very specific about who is doing what and when.

The MSSP and the client should clearly document in the SLA, the resources that can be accessed by the service provider. A client is entitled to confidentiality of its resources. Allowing the service provider to access its valuable resources is itself a risk. Therefore, in the SLA, the client must ensure that the MSSP has sufficient access to execute the contracted work.

The SLA should also specify the allotment of work by names along with contact information in the case of an attack. Depending on the kind of attack and the extent of damage, the MSSP's respond either by simple notification to full responsibility for incident handling. The SLA is an essential and binding document that outlines the contractual agreement between a client and MSSP.

The Future of MSSP

Outsourcing security technologies, infrastructure, services and management to outside providers is a hot trend that's only going to get hotter in the years to come. It is one of the fastest growing markets in IT with more than $250 million worth of VC-fed managed security startups in the last year. International Data Corporation (IDC) projects the worldwide market for information security services to grow to $16.5 billion by 2004 from $4.8 billion in 1998.

Microsoft and other major software manufacturers are testing fee-based or subscription oriented services that would allow their clients to use some of the flagship applications through the Internet. These services raise questions of additional security measures for the big corporations.

It is estimated that there are more than 80 million households that are linked to the Internet in the United States alone. This, combined with hundreds of millions linked to the Internet in the rest of the world, makes everyone vulnerable to cyber attacks. As the Internet users increase in numbers, there will be more services offered and more locks would need to be put in place for securing valuable resources.

References

DeJESUS EDMUND X., Ph.D. "Managing Managed Security", Jan.2001, URL: http://www.infosecuritymag.com/articles/january01/cover.shtml(03/02/2001)

Dr. Goslar Martin, *ZDNet Developer*, "Choosing trustworthy managed security services", Dec 05, 2000, URL: http://www.zdnetindia.com/techzone/enterprise/stories/8714.html (03/03/2001)

Trudeau Chris, DigitalMoJo Inc., "Managed Security Offerings, What to Look For", August 2, 2000, URL: http://www.techlinks.net/article.cfm?articleurl=8100232045 (03/03/2001)

Van Wyck Kenneth, CTO, Para-Protect, "Managed Security: Boom or Bandwagon?", June 2000, URL: http://www.infosecuritymag.com/articles/june00/departments3_on_the_cutting.shtml-security (03/05/2001)

Foley Mary Jo, Special to CNET News.com, "Microsoft mulling fee-based services", March 6, 2001, URL: http://news.cnet.com/news/0-1003-201-5038584-0.html?tag=cd_pr (03/06/2001)

This article was written by staff at the SANS Institute, a cooperative research and education organization, "Managed Security Services: Are They Right for You?" http://www.101com.com/securitysolutions/article.asp?ArticleID=1827- (03/06/2001)

The Yankee Group "Managed Security Outlook" (2000) http://www.yankeegroup.com/ (03/06/2001)