Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Outsourcing

The Internet has become an integral means of doing business over the past few years, making information one of the most valuable assets companies possess. As a result, companies are now forced to find ways to secure that asset. There are three ways to accomplish the security of the company's assets. The company can perform all tasks inhouse, hire an outside company or companies to perform all security related tasks, which is outsourcing, or some combination of the two. The primary focus of this paper is outsourcing sec...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Security Outsourcing
GSEC Practical (v.1.2e) (December 2000)
Jonathan S. Faile
Aug 25, 2001

Overview

The Internet has become an integral means of doing business over the past few years, making information one of the most valuable assets companies possess. As a result, companies are now forced to find ways to secure that asset. There are three ways to accomplish the security of the company's assets. The company can perform all tasks in-house, hire an outside company or companies to perform all security related tasks, which is outsourcing, or some combination of the two. The primary focus of this paper is outsourcing security services and therefore most of the discussion will reflect that, though some mention of the other two options will be put forth.

Outsourcing can be simply defined as an arrangement in which one company provides services for another company. These services are ones which typically could be handled in-house, but which are for various reasons turned over to another company or companies. It follows then that security outsourcing can be defined an arrangement in which one company provides security services for another company.

Information Security

The security of information involves the assurance of three key principles: confidentiality, integrity, and availability (BS 7799, 1999). If this assurance is achieved, then the information has been secured. The best way to achieve this is by implementing what is known as defense-in-depth. This principle states that to secure a network, several layers of defense must be present. Most organizations have implemented one level with a firewall, though insiders, viruses, and knowledgeable outsiders can easily circumvent these. Other measures must be taken to properly secure a network. Anti-virus software can limit the threat of viruses and a good intrusion detection system can be effective in detecting and neutralizing malicious activity. Configuration management with an established baseline coupled with regular auditing and backups will be effective in detecting and mitigating any successful intrusions or unauthorized activity. Some of these methods are part of the incident response program, which is also utilized to deal with legal issues arising from unauthorized activity such as forensic research and the chain of custody. Finally, for these tools and techniques to be effective, they should be defined clearly in the company's security policy.

The steps mentioned above come with a price however. Hardware and software must be purchased, often at great expense, to provide a sound security architecture. Security and information technology professionals must be hired to properly implement, maintain, and monitor the technology. Furthermore, technology is changing at a very rapid pace nowadays and it is crucial that the professionals keep up with changes, which requires that they be trained in the new technologies. Also, as technology moves forward,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

previous technology becomes outdated and thus security hardware and software must also be continually updated.

MSSPs

Managed security service providers (MSSPs) are companies that specialize in one or more aspects of providing security services for other companies. The range of these companies vary greatly, from the Big 5, which are large companies that offer just about every service, to smaller companies that may provide one service such as managed firewalls. Dejesus (2001) reported that the Yankee Group was tracking over 80 of these companies. As the market grows, more MSSPs are springing up such as Securify and The Mountain View with other established companies such as Cisco coming onboard as well (Network World). At the very least, those companies seeking outsourcing solutions will have a wide selection from which to choose.

Why Outsource?

There are many things to consider when deciding to outsource security or to keep it in-house. The difficulties associated with implementing defense-in-depth, hiring and training of highly skilled professionals, how to retain those individuals, cost, continual technological advances, increasing threat from outsiders (hackers and crackers), legal considerations, control, and peace of mind are all considerations. The complexity of these issues in implementing security has led to a boom in security outsourcing as many companies are beginning to seek the outsourcing solution. Indeed, Matthew Kovar of the Yankee Group stated that "Companies realize that they are not security companies and do not possess the core competencies to implement a holistic approach to security" (Pallack, 2001).

It is very difficult today to find qualified personnel to fill key positions in the security field. Tuesday (2001) stated "The market for security professionals is very tight at the moment, so it's difficult to find good people". Security is still an emerging profession and the supply of qualified personnel has yet to catch up to their demand. If a company is able to find qualified personnel, Breakaway Solutions noted that highly skilled personnel can command $100K-$120K per year, and many larger companies need more than three of these people. Therefore, even if a company can find qualified personnel, they may not be able to meet their salary demands.

When a company is able to hire qualified personnel, they will require training as advances in technology are made, which will further increases the cost of hiring personnel. Goslar (2000) noted that experienced and well-trained security professionals are hard to find and expensive to retain. They also might not like the hours they are working, since security is a 24/7 job. After they have received proper training, they become more marketable. As Tuesday noted, the market is very tight now and security professionals are in great demand. As such, they will not have difficulty landing a position with a company, perhaps an MSSP, which can meet their demands. Additional compensation in the form of money and benefits will be required to retain these personnel. Otherwise, the company will have to hire someone to replace them. It is likely that any replacement will need additional training and then the cycle starts over again.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Technology is rapidly advancing and security techniques and technologies along with it (Goslar, 2000). VPN equipment, IDSs, firewalls, routers, operating systems, penetration testing tools, and DNS are a few of the technologies that security professionals must be able to keep up with and learn inside and out. When it comes to IDSs, Michael Rasmussen of the Giga Information Group of Massachusetts stated, "IDS systems require care and feeding by experts, or you will not get anything out of them". IDS management should be left to the experts (Fonseca, 2001). Indeed, all of the technologies involved in security require vast amounts of knowledge and expertise to properly utilize them. To keep pace with these, any in-house staff will require substantial training funds, not to mention the money required to purchase the products and keep them up to date.

The threat of outsiders is also increasing. A multitude of sites are currently on the Internet, which are available for script kiddies. These sites allow for point and click attacks, requiring no knowledge of the underlying technology, only knowledge of how to use the Internet. They are capable of launching attacks such as a syn flood denial of service and the like which can take down a network and thus compromise availability. One example of this real threat is the attack on GRC.com, a security information site. Steve Gibson, who is a recognized security expert and runs the site, discovered that it was a 13-year who took down his site for some time before he was able to get it back online and working properly (Gibson, 2001). He went on to say, "Nothing more than the whim of a 13-year old hacker is required to knock any user, site, or server right off the net". However, script kiddies are generally limited by the tools available online and therefore do not constitute a high threat level, at least not until more sophisticated tools are placed at their disposal. It is the more advanced hacker that is the main reason companies need defense-in-depth. Skilled hackers utilize methods that are not public knowledge, often creating their own tools, discovering new holes to exploit, and even creating sophisticated new viruses. The recent Defcon hacker conference in Las Vegas can be considered an indication of the seriousness of the hacker threat. While some hackers have no malicious intent and will even let a company know if they find weaknesses, many are not and will try to break into your systems with some malicious intent.

Incident handling is very technical, involving disciplines such as forensics and chain of custody, and is essential for security. If a company doesn't have the staff with the expertise in-house, another possibility is calling the FBI. However, according to Mayor (2001), a lot of anxiety still exists among executives over calling the FBI. They are worried about the publicity and disruption of operations. The FBI is working hard to reverse this conception, but as it stands now, most companies will seek other alternatives. This is where an MSSP providing such services can be extremely useful. If they are already monitoring a network and an intrusion occurs, they have procedures and expertise in place to deal with the event rapidly.

Cost is a very important factor in deciding whether to outsource security. An advantage some MSSPs posses here is that with their size, they can offer economies of scale and thus set modest prices for their services that even smaller budgets can afford (Dejesus, 2001). As mentioned previously, the cost of in-house expertise in the form of salaries and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

training for security professionals can be very costly. Security hardware and software also can get to be quite expensive and at the rate technology is moving, they have to be continuously upgraded which drives costs up even further.
Of note also is that many companies, especially smaller ones, are not able to hire the security professionals they need, given their limited budgets. Instead, they either rely on their IT staff to perform security functions or have an understaffed security office which doesn't have the necessary manpower to properly perform security functions (Gaudin, 2001). However, security is a full time responsibility and will suffer if not properly run. These companies spread themselves thin and as a result create more problems. If more time is allocated to security by IT staff, then other responsibilities, possibly some core business functions, will begin to suffer. Also, improper staffing may also lead to security flaws that may open the company's network up to attack. By outsourcing these services, a company can get back to its core business functions and stop opening itself to vulnerabilities by spreading its resources too thin.

Now might be an excellent time to outsource while the market is down. As profit margins get tighter, companies are forced shrink their budgets. This could mean that the company may not be able to afford salary and training demands of its staff. Also, hardware and software upgrades and purchases may have to be put on hold until the market gets better, all of which create significant security concerns for the company. As noted previously, since MSSPs create economies of scale, they are able to offer affordable prices to their clients. Personnel, hardware and software are all offered, so an MSSP should be able to address these concerns and might possibly be the way to turn during a slumping economy.

Some Outsourcing Concerns

According to Network World 500's annual survey of 500 network executives, security is what keeps them up at night. Security and hackers ranked as the number one concern (Gaspar, 2001). Keeping up with rapidly changing technology and finding qualified technical personnel also ranked near the top. Depending upon the level of outsourcing, one or all of these fears can be assuaged. This is because when the MSSP takes over security operations, it becomes their responsibility. They are the ones who have to hire trained security personnel, keep up with the rapidly changing technology, and worry at night that they are performing up to standards or else they will lose their clients. They probably do not worry as much as a company whose core business function is not security however. For these reasons, bringing in an MSSP with a good reputation should bring peace of mind to any CEO or CIO.

Many executives feel uncomfortable about handing over their networks, and thus their sensitive data, to a managed security service provider for monitoring. The term managed implies that the control over some operation is placed beyond the control of the company. Therefore, with a managed security service, control over security functions will be turned over to the company or companies providing the security services. For those who are uneasy about turning control of their company, this doesn't have to be a major concern. This is an area where the Service Level Agreement (SLA) is very important. It is a contract between the company and the MSSP, which spells out in detail certain aspects of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the relationship, to include access to information. Once the level of access has been established, information disclosure agreements can be made. Negotiation between the company and the security provider concerning this should be able to bring about a good SLA that will eliminate most of the fears of handing over the company's sensitive data.

Selection Process

Once a company has decided to outsource its security, the first step is to determine exactly what will be outsourced and what will be kept in-house. Then, the company should research those MSSPs that provide the required services. This research should include but not be limited to such things as the MSSPs financial situation, reputation, size, cost, location, and comfort level. If an MSSP goes bankrupt while providing security services, this can have dire implications for all of its clients. They will be left to fend for themselves, whether they have the resources to or not. Therefore, it is crucial that only financially sound MSSPs be considered.

Reputation is also a key issue because the MSSP will have access to your company's sensitive data and be responsible for your network. Care should be taken in seeking out references from current and former clients of the provider in question before serious negotiations occur.

The size of the company can also come into play. Some companies feel more comfortable dealing with smaller providers where service may be more personable. Other companies may prefer the assurance that comes with larger providers like the Big 5.

Cost is listed for obvious reasons. If the company cannot afford the services offered then it will have to keep searching for providers. It is not likely to be a hindrance though. Larger providers are often able to offer affordable prices due to their size. Other providers just entering the market may also offer very reasonable prices as they try to gain market share. Through a little research, a company should be able to come up with several alternatives.

Location can also be an important factor. Some companies, mostly the smaller providers, are limited by geography as to whom they are able to serve. Other larger providers can provide the means for their clients to hook into a central location where the provider is able to monitor all of the networks it is responsible for, eliminating geography issues.

As important as these factors are, the level of comfort with the provider may be the most important. This factor incorporates all of the others, but goes one step further. Before contract negotiations take place, management should visit with the provider in question and meet the people who will be monitoring its networks, perhaps take a tour of the facility, and meet with the management team. This process should give some indication of the business culture and provide some indication as to how provider conducts business.

Once a suitable provider has been identified, contract negotiations can begin. Specifically, the SLA will be negotiated at this time. This contract identifies access to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

your systems, behavior during an attack, and performance criteria (Dejesus, 2001). It can limit the amount of access the provider has to your sensitive data, but care must be taken so the provider has enough to perform its job properly. The SLA will also specify roles and responsibilities during an attack. Some things to consider are: who will handle incidents and to what degree, what the time frame is for response and reporting, what the response will be, and who the contact personnel are. Performance criteria are also part of the agreement. The purpose of this is to provide the client with some quantitative measurement of the provider's performance. Once these are specified, some knowledgeable in-house staff should be charged with monitoring adherence to the SLA.

Summary

Managed security is a rapidly emerging business. Revenues from this form of business are expected to reach into the billions in the next few years (Pallack, 2001). The reason behind this is that the Internet has become an integral means of conducting business. Once a company goes online, its most important asset, information, becomes vulnerable and the company is forced to mitigate this threat. However, it is very difficult to perform security properly. New technologies that are increasingly complex, finding and retaining qualified security professionals, and the difficulties associated with implementing defense-in-depth all go a long way towards the migration to managed security providers. These providers can eliminate the headaches associated with finding, hiring, training and retaining qualified personnel, as well as purchasing hardware and software and the constant upgrades associated with them. The tools and personnel to use them are already in place with an MSSP. With some of the larger providers, economies of scale are gained and they are able to offer reasonable pricing to the client, which can ease financial considerations. As a security entity, they also understand the fundamentals of information assurance and defense-in-depth and are fully capable of deploying tools to assure each. It could be said that they provide economies of skill as well (Dejesus, 2001). Since they handle some form of monitoring for multiple clients, any knowledge gained from an attack on one client's network can be applied and used to protect other clients.

Bibliography

1. BS 7799 British Standard, Part 1, Information Security Management. 1999.

2. Gaspar, Suzanne, Security Concerns Dominate NW500 Survey. May 07, 2001.
URL: www.nwfusion.com/research/2001/0507feat2.html

3. Network World. Managed Security Services are Gaining New Players. April 02, 2001.
URL: www.itworld.com/Man/3886/NWW010402119109/

4. Dejesus, Edmund X., Managing Managed Security. January 2001.
URL: http://www.infosecuritymag.com/articles/january01/cover.shtml

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5. Tuesday, Vince, Security Outsourcing: Don't Bet on it Yet. June 11, 2001.
URL: www.computerworld.com/cwi/story/0,1199,NAV47_STO61232,00.html

6. Fonseca, Brian, Cutting Back on False Alarms. June 15, 2001.
URL: http://www.inquiry.com/pubs/infoworld/vol23/issue25/010618hnintrusion.asp

7. Pallack, Chris, Security Outsourcing Set to Soar. May 23, 2001.
URL: http://www.it-analysis.com/article.php?id=1237

8. Mayor, Tracy, Break Glass, Pull Handle, Call FBI. June 01, 2001.
URL: http://www.cio.com/archive/060101/fbi.html

9. Gibson, Steve, The strange Tale of the Denial Of Service Attacks Against GRC.com. July 04, 2001.
URL: http://grc.com/dos/grcdos.htm

10. Breakaway Solutions, Examining Network Security Outsourcing.
URL: www.breakaway.com/pdf/pdf_file/outsourcing_security_whitepaper.pdf

11. Goslar, Dr. Martin, Choosing Trustworthy Managed Security Services. December 05, 2000.
URL: http://www.zdnetindia.com/techzone/resources/security/stories/8713.html

12. Gaudin, Sharon, Spending on the Rise. January 29, 2001.
URL: www.nwfusion.com/research/2001/0129feat.html

© SANS Institute 2001 - Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**