Global Information Assurance Certification Paper

Technologies That Require IT to Extend the Layers of Defense

SANS Security Essentials (GSEC) Practical Assignment
Version 1.4
Charles Tholen
May 14, 2002

Introduction

This document looks at how currently established layers of defense need to be extended because of technologies being implemented or used in corporate IT. It is intended to provide information to the IT professional who has a base understanding in security principles. Each area can be looked at much deeper individually, but have been presented here to provide insight to potential areas of risk that exist in every corporate network knowingly or unknowingly. For each technology, I will provide a description of the technology, risks related to the technology, and methods for reducing that risk.

Defense in Depth

Besides having to keep up with the every growing number of exploits and vulnerabilities, Corporate IT has to consider the new technologies being implemented in their environments from a security perspective. IT also has to consider the new technologies that are used by employees for either personal or business use. These technologies may or may not have been implemented by IT. These new technologies have the effect of creating holes in their existing defense strategy.

The typical strategy of Defense in Depth (DiD) "combines the capabilities of people, operations, and security technologies to establish multiple layers of protection--analogous to protecting a home with multiple defenses. These defenses may include a strong lock at the front door, secured windows, an electronic home security system, bright lights on the outside, a neighborhood watch program, and a dog that barks at people who walk near the home. An intruder must circumvent these defenses in order to gain unauthorized entry to the home. With DiD, the objective is to implement defenses at multiple locations so that critical enclave resources are protected and can continue to operate in the event that one or more defenses are circumvented."[1]

It is important to understand for IT to understand how new technologies impact implemented security strategy. The technologies discussed in this document have the effect of extending the security requirements of the traditional layers of defense implemented by IT to cover the holes created by these technologies.

Traditional Layers of Defense

In taking step to protect corporate information resources, IT has attempted to provide Defense in Depth by implementing various layers of defense across their enterprise. Traditionally, the layers of defense IT implements look to defend the perimeter, the network, and hosts.

Firewalls are typically used in defending the perimeter. By definition, "a firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to."[ii] This provides the first layer of defense from those outside the protected network and filters what external resources can be accessed from the inside.

Network intrusion detection tools are used for protecting the perimeter and the internal network by watching packets for signatures of know exploits. New technologies for IDS are becoming available that include behavior monitoring and anomaly detection. These systems "are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries."[iii] Servers and workstations are typically protected by anti –virus software and host based intrusion detection systems. Host based intrusion detection "systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable."[iv] Figure 1 is a logical representation of these typical layers of defense.

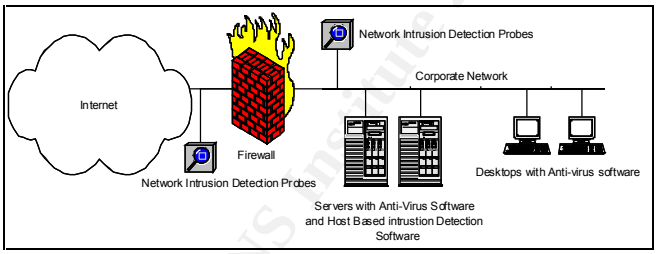

Figure 1 - Typical Layers of Defense

As a test of all these systems, it is common for Vulnerability Assessment tools to be used to discover areas of weakness within the environment. Not only are these types of technologies being relied on, but they are also typically covered under current Security Policies. These cover the risks that are at the top of mind with IT. However, there are technologies being employed by IT and users that are extending the security needs with in these layers of defense.

Extending the Layers of Defense

The traditional layers of defense are being extended and circumvented by new technologies being implemented by IT or, unknown to IT, by end users inside the

organization. These technologies need to be detected, understood and addressed to avoid potential risk and even the defeat of current security measures. What is common in the areas covered is that they are typically not specified in Security and Usage policies and are used in most every company whether authorized or not. The first two areas of concern, VPN and Wireless Networking, are commonly implemented by IT while the remaining three areas, Instant Messaging, Peer Files Sharing tools, and Web Based email typically are not but are still commonly used.

Virtual Private Networks

With an increasing number of traveling and home office based employees, IT has been deploying various technologies to facilitate connections back to corporate resources. The most notable has been Virtual Private Networks, or VPNs. A VPN is "one or more WAN links over a shared public network, typically over the Internet or an IP backbone from a Network Service Provider (NSP), that simulates the behavior of dedicated WAN links over leased lines."[v] VPNs allow for a secure network connection from a remote host to be made to a secure corporate network by tunneling across a public network. This is accomplished by using a client creating a secure, encrypted channel to a server or device sitting on the company's perimeter. This channel makes the client a part of the corporate network. Figure 2 is a logical representation of a VPN.

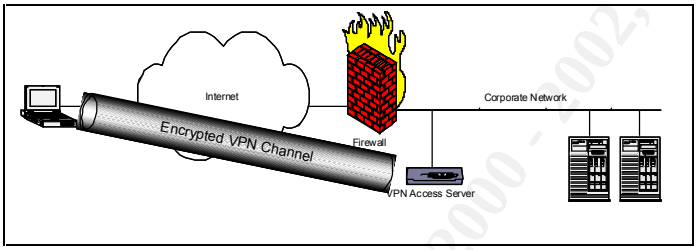

Figure 2 - Logical Representation of a VPN

Through the VPN client, the employee now is able to use corporate resources as if they were sitting in the office. While fitting the needs of the remote employee, it is common for this to create holes in a company's layers of defense.

All too often VPNs are implemented in a rush to meet a business need and neglected from a policy standpoint. This leaves IT with no legs to stand on when trying to implement additional security after the initial implementation. This is especial important with the use of VPNs. While the connection made to the corporate network is encrypted, the level of overall protection is dictated by how well the remote machine is protected. Remote machines need to be scrutinized harsher because they do not benefit from the layers of defense implemented inside the corporate network. The typical use of VPN is by home users or traveling users. This means that the remote machine is connected to broadband or dial up public networks and the VPN connection is made across the Internet.

The types of risks faced by machines directly connected to the Internet as discussed by CERT are:[vi]

1. Trojan horse programs
2. Back door and remote administration programs
3. Denial of service
4. Being an intermediary for another attack
5. Unprotected Windows shares
6. Mobile code (Java, JavaScript, and ActiveX)
7. Cross-site scripting
8. Email spoofing
9. Email-borne viruses
10. Hidden file extensions
11. Chat clients
12. Packet sniffing

The risks stemming from the remote computers are compounded when the VPN client allows Split Channels. A Split Channel occurs "when a VPN client can connect to both secure sites(via VPN) and non-secure sites, without having to connect or disconnect your VPN connection. The client can determine whether to send the information over the encrypted path, or to send it via the non-encrypted path."[vii] One of the most common implementations of VPN is through the native capabilities of Windows NT/2000 utilizing RRAS. The Microsoft implementation does allow for a secure encrypted connection and ease of access to corporate resources. However, one key configuration option allows for a Split Channel to occur. Figure 3 shows the setting for controlling if communication will be allowed outside the VPN connection.

Figure 3 - TCP/IP Setting for Microsoft's VPN client

Removal of the check in the check box allows the Split Channel. This puts the corporate network at risk since the remote systems can now be used as a conduit to reach corporate network resources. All of the risks associated with the remote machine are now extended to the corporate network. Tracking down incidents occurring from a VPN connected machine can be very difficult. From the view of the corporate network, incidents will be originating with the remote machine. Getting information beyond that can be difficult because it will require getting the information regarding connections from the ISP the

employee uses to connect to the Internet. To combat these risks IT needs to extend their layers of defense.

There are several ways IT can extend their layers of defense to make sure they have a securely implemented VPN and not compromise the needs of the remote employee. First, IT needs to makes sure VPN and remote access is covered under their Company's Security and Usage Policies. Policy needs to include a method for authorizing the use of remote access, criteria for the system that will be connected (preferably a company provided pc or laptop), and usage while being connected. See http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.doc for an example of such a policy statements. Adding this to Policy paves the way for being able to implement solutions to protect corporate resources. Next, IT needs to maintain proper configurations for the machines being connected. This should include the use of a third party VPN solution from vendors such as Cisco or Checkpoint. Finally, implement host based tools for protecting the remote system. Anti-virus software needs to be implemented and kept up to date. Personal firewall software should also be used and configured deny any communication not explicitly denied.

Wireless Networking

Corporate networks are being broadened by Wireless Networks. This further extends the layers that need protected inside the network. As defined Wireless Networking is "a computer network where there is no physical connection (either copper cable or fibre optics) between sender and receiver, but instead they are connected by radio."[viii] This is done by having these wireless devices communicate amongst themselves in a peer configuration or by using an Access Point for them to participate on the network. Access Points act as hubs for all of the wireless nodes to connect through to connect to the rest of the corporate network. Examples of wireless devices are Handhelds, Laptops configured with wireless network adapters, and print servers. Figure 4 shows a logical representation of a wireless network connected to a corporate network.

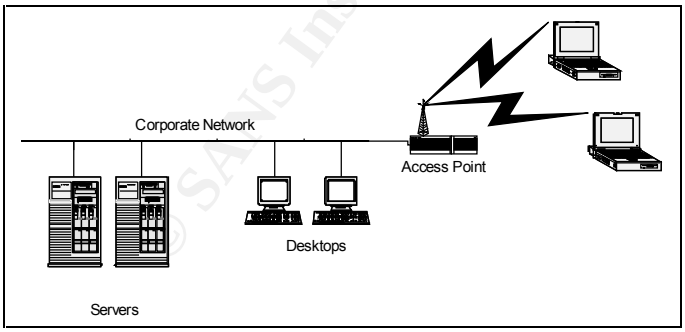

Figure 4 - Logical Representation of a Wireless Network

Wireless Networks are being used in more mainstream uses than just access to corporate networks. Recently, "Best Buy suspended use of wireless cash registers over concerns that eavesdroppers could obtain credit card numbers and other customer data by sitting in the parking lot with the right equipment."[ix] Retail registers is just one example at the growing use of wireless networking. The most common wireless implementation is the

802.11 standard. A detailed discussion of the 802.11 standard can be found at the IEEE website, http://grouper.ieee.org/groups/802/11/main.html . Some security provisions were included in the 802.11 standard. The first measure is SSID, or Service Set Identifier. SSID is the identifier for a specific wireless network. All the nodes connecting to this wireless network including the Access Points must have the same SSID. 802.11 also specifies WEP, or Wired Equivalent Privacy. WEP allows for the encryption of the signal between the clients and the Access Points using a 40bit or 128bit key. Access Points can also compare the MAC address of the client trying to connect with an allow list to further help secure the environment.

Even with the security items specified by the 802.11 standard, there are still considerable risks to implementing Wireless Networks. One of the biggest risks is installing Access Points with default configurations. This typically occurs when the wireless solution is put into place to fill an immediate need, in pilot implementations, or by non-IT personnel. The security vulnerabilities inherent with default installations is that MAC access lists and WEP are disabled. Also, the default SSIDs for various vendors are widely known. Outsiders can easily find such an environment quickly and become a node on the network. With WEP disabled, it is also easy to eavesdrop on the network communications being broadcast through the air. This is basically packet sniffing the wireless network. This is of great concern for commercial uses of wireless networks, like Best Buy's cash registers. In "Tales of a White Hat War Driver," Alan Rothberg details his study of eavesdropping on wireless networks. His story can be found at http://www.oreillynet.com/pub/a/wireless/2002/03/29/wardriver.html. There are several tools, like NetStumbler and Airsnort, that are focused on identifying details about wireless networks and sniffing the packets of that network. This is all a hacker needs to gain a connection. Once a hacker has access to the wireless network, they have access to the rest of the corporate network unless layers of defense are extended to cover the wireless environment.

There are several ways IT can extend their layers of defense to make sure they have a securely implemented wireless networking technologies. First, IT needs to makes sure Wireless Networks are covered under their Company's Security and Usage Policies. Policy should include approval mechanisms for implementing, acceptable use, and proper security configurations. Creating the policy statements will help in properly implementing these technologies so security issues are looked at and designed into the implementation. From the technical perspective, properly securing a wireless network with implementing the security features built into the 802.11 standard. However, a more secure environment can be built by going beyond these built in features. By placing the wireless network in an untrusted part of the network, secure connections can be made by utilizing VPN technologies. The key is to separate the encryption from WEP. Once the wireless node has made a connection into the wireless network, a VPN client is used to make the secure connection into the protected corporate network.

Figure 5 shows a logical representation of a wireless network connected to a corporate network through a VPN.

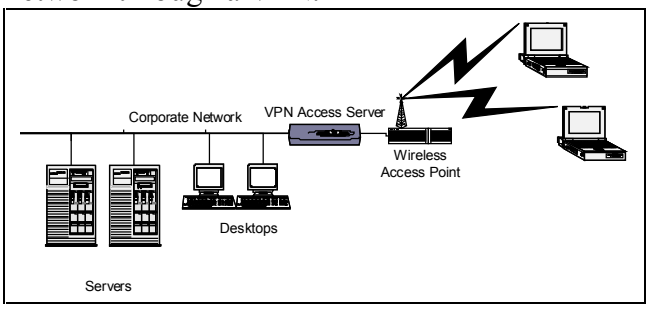

Figure 5 - Wireless Network using VPN

This will prevent the ability for the hacker to gather corporate proprietary information through eavesdropping. Also, if a hacker does gain a connection to the

Instant Messaging

By definition, "Instant Messaging (IM) is an Internet protocol (IP)–based application that provides convenient communication between people using a variety of different device types. The most familiar today is computer-to-computer instant text messaging, but IM also can work with mobile devices, such as digital cellular phones, and can incorporate voice or video. Although there are a number of free Internet-based messaging services, IM is a feature that carriers can offer to increase customer loyalty and add value to their service offerings."[x] Instant Messaging allows for people to use a client to send messages to others using the same client. Clients know the status of other clients by connecting to a server that maintains a directory of other connected clients and their status. The client can be used for chatting, sending messages, and the transferring of files. The most commonly used IM clients are AOL-IM, ICQ, Yahoo IM, and MSN Messenger. A more complete list and reviews can be found at http://www.cnet.com/software/0-5566362-8-8481018-1.html . Most commonly these tools are used for text chat to communicate with family, friends, or meeting new people. Besides personal chatting, some companies are finding business uses for these technologies. This includes inter-office communication with remote employees or between project team members. Some companies implement instant messaging for a direct, real time connection to customers to enhance customer service capabilities.

Whether for personal or business use, instant messaging is growing in popularity in the workplace. This presents several security risks to the corporate network. The IM clients themselves are constant targets for hackers trying to leverage existing vulnerabilities and new exploits. Typical vulnerabilities include being susceptible to Denial of Service attacks, allowing the execution of code, and transferring of malicious files. IM clients have the potential for providing an access point to the rest of your corporate network. Another security vulnerability with IM tools is the ability to communicate company proprietary and personal information to people outside the organization. This could be knowingly or unknowingly. IM tools do not provide for a secured messaging environment and the packets can be sniffed off the wire. A good source for reading more about IM related risks is http://www.business2.com/webguide/0,1660,55212,FF.html .

There are several ways IT can extend their layers of defense to make sure that the risks of Instant Messaging are minimized. First, IT needs to makes sure IM tools are covered under their Company's Security and Usage Policies. Ideally the usage of IM connected to public directory servers should be prohibited. Host based tools can be implemented to monitor for the loading of the various IM clients and can notify administrators or kill the application. If IM technology is required for business needs, usage could be permitted from internally implemented directory servers. Companies that need external communication through IM should look into implementing auditing software to monitor its usage. FaceTime's[xi] IM Director is an example of a solution that provides such functionality. This level of auditing can also be obtained through keystroke loggers. Besides technical remedies, end user education can play a key role in reducing risks associated with Instant Messaging.

Peer File Sharing Tools

Peer File Sharing tools, such as Gnutella, are tools that allow the sharing of files between computers. These tools "facilitate the location and exchange of files (typically images, audio, or video) amongst a large group of independent users connected through the Internet. In these systems, files are stored on the computers of the individual users or peers, and exchanged through a direct connection between the downloading and uploading peers, over an HTTP-style protocol."[xii] The client connects to a host cache for doing search for files and IP addresses of clients. The client also acts as a server for files and posts the active IP address to the host cache. When you select a file to download you connect to the host serving the file. If this host is not directly reachable, the host will initiate a connection to you.

This highlights the main problem of bypassing IT standards and security measure with these tools. Tools like Gnutella are designed to bypass firewalls by being able to use commonly allowed ports, like port 80, to make the out bound connection to the requesting host. This makes usage very difficult to stop. A discussion for configuring Gnutella to work through firewalls can be found at http://www.gnutellanews.com/information/firewalls.shtml . Besides the ability of bypassing firewalls, there is also the matter of the files being downloaded. These files can come from questionable origin and could contain virus or trojan horse type programs that put your corporate network further at risk. Files being downloaded can include pornography, warez, MP3s, and other files that could make the company and the employee liable or subject to prosecution. Also, company proprietary information could be shared out to the world either accidentally or intentionally. Peer File Sharing clients are a constant target for hackers trying to leverage existing vulnerabilities and new exploits. Typical vulnerabilities include being susceptible to Denial of Service attacks, allowing the execution of code, and transferring of malicious files. IT needs to analyze the overall risk to the organization and extend their existing layers of defense to include Peer File Sharing tools.

There are several ways IT can extend their layers of defense to make sure they minimize the risks of Peer File Sharing Tools. First, Peer File Sharing Tools need to be covered under the company's Security and Usage Policies. There is no business need for using these tools and they should be prohibited. Enforcement of such policies is also important. From a technology standpoint, host based tools can be used to monitor for the execution of tools like Gnutella and can allow for the administrators to be notified or the application killed. In addition to technical remedies, end user education will play a key role in reducing risk of these tools. If the users truly understand the risks they are introducing, they may indeed help with the effort. If they do not buy in on the problem, the challenge will be that much greater for IT.

Web Based Mail

By definition, Web Based email is "an email account that is accessed through a Web browser. The interface is implemented as a Web site that provides access to the various functions like reading, sending or organizing messages. Emails are typically not downloaded to the user's computer but stored on the Web-based email service provider's servers."[xiii] Web Based Email allows the user to send and receive email over the Web using a standard web browser from anywhere, included company issued machines. The Web browser is used to connect to a web page hosted by the web email provider. The most common is Hotmail/MSN Mail and Yahoo Mail. Most ISPs today also allow their customers to access their email over the web. What is notable about Hotmail/MSN and Yahoo, is that it is freely available and has no verification of the information entered when creating an account. This essentially allows for completely anonymous email accounts.

Like the other areas covered, usage of Web Based Email is typically not covered by policy. Employees use Web Based Email to maintain privacy or to bypass policy cover acceptable usage of email. Just by being accessible via the web makes it very difficult to monitor or track its use. This means that improper communication can take place under the noses of IT. This communication can be competitive information to rivals or even inside information that could affect the stock market. Another problem with Web Based Email are the emails that are received. The amount of spam associated with Web Based Email is enormous and does not get screened by the systems that IT may use for the company's email systems. Virus and worm code can easily be transmitted from these email services, especially since everything is web based and allows scripting code in the web page to be executed. These risks need to be weighed against the company's concern for personal privacy and the results reflected in the company's defense strategy.

There are several ways IT can extend their layers of defense to make sure they minimize the risks of Web Based Email. First, Web Based Email needs to be covered under the company's Security and Usage Policies. There is typically no business need for using these tools and they should be prohibited. This addition to policy paves they way to implementing measures for blocking the specific urls associated with Web Based Email. This needs to cover not only the personal use of but also the dissemination of company proprietary information. Getting detailed employee web usage reports can help track

down Web Based Email sites. Blocking the urls of known Web Based Email sites is the next step. If unable to block these sites, enforcing configurations of the web browsers to prevent script execution helps against malicious code embedded in email. In addition to technical remedies, end user education will play a key role in reducing risk of these tools. If the users truly understand the risks they are introducing by using Web Based Email, they may indeed help with the effort.

Conclusion

VPNs, Wireless Networks, Instant Messaging, Peer File Sharing, and Web Based Email are technologies being used pervasively in corporate networks today. The technologies in use may be known or unknown to IT and typically have not been included in security analysis and may circumvent the traditional layers of defense. The risks associated with these technologies are real and must be addressed by IT. This process begins with understanding the specific technology in question. This includes architecture, usage, detection, management, and methods of implementation. Next, the security risks need to be clearly understood. This includes not only risks to the corporate network, but also liability and information loss. Once these risks are understood, work can begin on security strategies to minimize the risks. Security strategies look to provide secure usage of the technologies or may even prevent their usage all together. Besides technical strategies, education can play a big role. This includes education of the IT professional and the end users. The most important factor in minimizing the risks is coverage in policy. Security and Usage Policies must be keep current with new technologies and should be in place before implementing technical security strategies. Policy provides the foundation for security strategies and allows IT to extend their layers of defense.

Resources

http://www.infosyssec.org/infosyssec/secvpn1.htm
http://www.extremetech.com/article/0,3396,apn=8&s=1034&a=13880&app=6&ap=7,00.asp
http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/WLO_Security_WP_LOWrez1.pdf
http://advisor.com/Articles.nsf/aid/MENGC001
http://www.business2.com/webguide/0,1660,55212,00.html
http://www.business2.com/webguide/0,1660,55212,00.html
http://www.wired.com/news/politics/0,1283,21498,00.html
http://advisor.com/Articles.nsf/aid/FRASS257
http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.doc
http://www.oreillynet.com/pub/a/wireless/2002/03/29/wardriver.html
http://grouper.ieee.org/groups/802/11/main.html
http://www.cnet.com/software/0-5566362-8-8481018-1.html
http://www.business2.com/webguide/0,1660,55212,FF.html
http://www.gnutellanews.com/information/firewalls.shtml

Bibliography

[i] McKenney, Brian. "Defense in Depth". Feb. 2001. URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm (Apr. 2002)
[ii] searchsecurity.com. "firewall". Dec. 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212125,00.html (Apr. 2002)
[iii] Elson, David. "Intrusion Detection, Theory and Practice". March 2000. URL: http://online.securityfocus.com/infocus/1203 (May 2002)
[iv] Elson, David. "Intrusion Detection, Theory and Practice". March 2000. URL: http://online.securityfocus.com/infocus/1203 (May 2002)
[v] Hsia, Alex. "VPN Demonstration". May 1999. URL: http://boulder.noaa.gov/noc/HPCC99/Alex/vpn/tsld002.htm (May 2002)
[vi] CERT Coordination Center. "Home Network Security". 2000 - 2002 URL: http://www.cert.org/tech_tips/home_networks.html#III (May 2002)
[vii] Mencik, Stephen. "Infrastructure & Network Security Expert(s):". April 2001. URL: http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid388798_tax285453,00.html (May 2002)
[viii] Howe, Denis. "The Free On-line Dictionary of Computing". Feb. 1995. URL: http://www.dictionary.com/search?q=wireless (May 2002)
[ix] Jesdanun, Anick. "Privacy Risks Grow With Wireless Tech". May 2002. URL: http://story.news.yahoo.com/news?tmpl=story&u=/ap/20020503/ap_on_hi_te/wireless_insecurity_3 (May 2002)
[x] International Engineering Consortium. "On-Line Education: Instant Messaging". 2001-2002. URL: http://www.iec.org/online/tutorials/instant_msg/ (May 2002)
[xi] FaceTime Communications. "Product Overview". 2002. URL: http://www.facetime.com/products.shtm (May 2002)
[xii] Saroiu, Stefan, et.al.. "A Measurement Study or Peer-to-Peer File Sharing Systems". Jan. 2002. URL: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf (May 2002)
[xiii] About.com. "Web-based Email". 2002. URL: http://email.about.com/library/glossary/bldef_web-based_email.htm (May 2002)