Global Information Assurance Certification Paper

Jeremy Miller
GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 1
March 23, 2004

Remote Users Working from Home – Are You Prepared?

TABLE OF CONTENTS

ABSTRACT

Bob works at home for a marketing company putting together marketing strategies for the upcoming year. His friend Jeff happens to work for a competing marketing company. One day Bob is talking with Jeff and mentions that he needs a faster PC. Jeff talks Bob into selling his PC to him for a cheap price. Bob, being the smart guy that he is goes through every single folder deleting all of the files that he doesn't want Jeff to have. Jeff brings the PC home and starts looking through the folders just to see what is installed and found all of Bob's files and was able to open and read every one of them. How was Jeff able to get all of Bob's files that he deleted? You wouldn't believe it but Bob forgot to empty his recycle bin before giving it to Jeff. If Jeff really wanted to be promoted and look good, he could use that information against Bob and possibly cost Bob's company thousands, if not millions of dollars. Even if Bob had emptied his recycle bin, Jeff could have hired a company to recover the data off of the hard drive.

The above example is just one of many risks associated with remote access. Teleworkers are on the rise and there looks to be no sign of it slowing down. According to Gaudin (2003), "There has been a 40% increase over the last two years in people working from home." Why such an increase? Technology has opened the door for employees to gain access to the same exact resources as if they were sitting at their PC in their office. Teleworkers save time and money by not having to travel to work. They now get to work out of the comfort of their own home. The teleworker's company saves money because they do not have to provide office space and in some cases they do not have to provide the teleworker with a PC. The sales force can be more efficient on the road because they have access to high speed internet in their hotel room and a VPN (Virtual Private Network) connection to the office. Ron Miller states (2004), "By 2008 households using broadband will double to more than 46 million." This also allows the teleworker to be much more efficient when working at home. There's no doubt that remote access favors both the teleworker and the company; so what's the big deal? Although working at home is attractive to business owners and employees, there is one thing to consider – Information Security! Opening the door for an employee to work from home also opens many doors in compromising information security. This document will provide the user community, security professionals, and business owners with practical knowledge on telecommuting and its associated risks. It will also serve as a resource and tool for mitigating risks by providing samples such as a remote access policy, remote access flowchart, remote user guide, and introductions to technical solutions for remediation.

RISKS

The risks of remote access affect any organization that has a business need to have VPN users connect to the company. Throughout this document the term

"PC" will represent both Laptops and PCs as the risks are the same for both. All risks mentioned below apply to both company owned PCs and employee owned PCs with the following exception:

"Employee Owned Laptop/PC's Not Sanitized Before Disposal"

This exception only applies to employee owned PCs, because company owned PCs should already have a disposal policy and procedure in place.

Files on Remote Laptop or PC are Compromised, Lost, Stolen or Not Sanitized

Files are truly one of the biggest areas of concern. Files contain important data such as business strategies, financial data, personal health information (PHI), etc. When users establish a VPN connection to the office, they have access to all of their files. They can map network drives to the server where files are stored and they are able to browse through *Network Neighborhood* or *My Network Places* to get to them. Once users open a file they have the ability to save either on the network or locally. They could store them on the hard drive, floppy disks, CDs, and now USB flash drives. Can security professionals assume that the employee will open the file from the network over the VPN and never store the file locally? Let's see, work on the file locally with no latency or work over a slower VPN connection, which would one choose? If the files are getting stored on the local hard drive then how as security professionals do we maintain the integrity and protection of the data? What happens if the laptop is lost? How would the data be protected? In the remediation section of this document I will walk through the entire remediation process and provide the tools and resources necessary to tackle such a daunting task.

An area often overlooked, when it comes to remote PCs, is the possibility of retrieving data from already formatted hard drives. There are a lot of tools and software packages available on the Internet that will recover data if a hard drive was damaged, files were accidentally deleted, or the drive was accidentally formatted. The Department of Defense (DOD) has a recommended approach or standard to ensure that all data is removed from writable media. This standard has been implemented in many software packages of companies that specialize in data recovery and data security. One of the many functions of this standard is replacing all addressable locations with a single character, its complement, and then a random character (Lsoft Technologies, 2002). The task of sanitizing all hard drives that host or at one time hosted company data can be very time consuming, but at the same time necessary to protect a company's data.

Media Improperly Handled

Media is a tough area and is extremely difficult to manage and protect. We live in times where more mobility is better. We want data available wherever and however we can get it. We want to be able to save it and retrieve it as quickly as

possible. Media can come in a variety of formats such as hard copies, CDs, floppies, and USB flash drives. Do we live in a paperless world? A lot of us techies would like to think so or at least hope we could. I don't know about you but I have a hard time keeping track of and organizing all the hard copies that I have. Yet, from time to time, I would still prefer to have a paper copy in front of me so I don't have to scroll up and down or keep changing my screen resolution so I can read more text at a time. Most people that have PCs at home have printers which, brings up an area of concern for VPN users because they can now print company documents at home. There are several security risks to look at. One is that anyone who visits the employee's home could potentially read the printed copies sitting out in the open or steal them. It could contain all different types of sensitive data such as financials, marketing strategies, and PHI. The same applies for all other types of media. All can easily be stolen or lost, which provides easy access to information.

Downloading and Installing Software Unapproved Software

Downloading and installing software from the internet is becoming more popular everyday. People are downloading all kinds of software such as programs, games, screen saver, plugins, etc… This area applies to the employee using a company PC or their home PC to connect to the company network. Downloading software from the internet is risky business especially if it is not a well-known software package from a reputable source. There is no guarantee that the software being downloaded and installed is safe and will not install unwanted features. For example, a hacker could have created some back doors in a software package that would allow him to connect to the PC later. The hacker could then launch attacks on other websites or PCs using the compromised PC. He could also use the PC for spam relay. Guess who would get accused of the attack? In most cases it won't be the attacker. An employee who has teenagers using the same PC used for connecting to work would be even more risky. I have heard many stories from co-workers who had to take their home PC to someone to reformat the hard drive because their children either opened an attachment that had a virus or their PC was so messed up from all of the programs they had downloaded and installed. There is also the risk of visiting malicious websites. This could happen to almost anyone, especially when clicking on a lot of links doing research. There is a high probability of spyware and adware being installed without the consent of the user and without the user even being aware of it.

Use of Wireless Networks

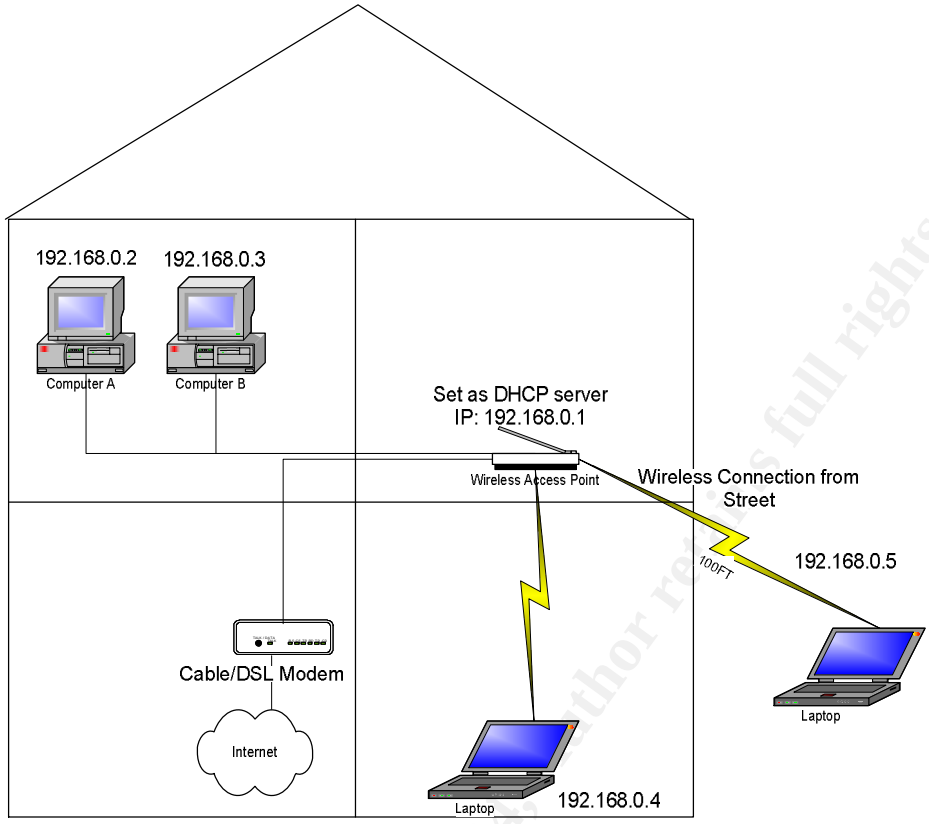
Wireless is growing rapidly in the home as well as in other areas such as hotels, cafes, and airports. These places provide a wireless router or access point, which provides users who have wireless adapters access to the internet. Wireless routers in these areas provide easy access to the Internet, making it easy to gain access to company email and allowing the user to VPN into the company network. The downside, however, is everyone using that same network

can now potentially probe the remote PC for vulnerabilities. If the PC is un-patched it might be easy for an attacker to compromise the PC. The same holds true for employees working at home using wireless routers. Most wireless routers come with an un-secure default configuration. Anyone that has a wireless adapter can drive up next to a house or company and try to connect to the access point inside. Jeanne-Vida Douglas (2002) supports this theory by stating:

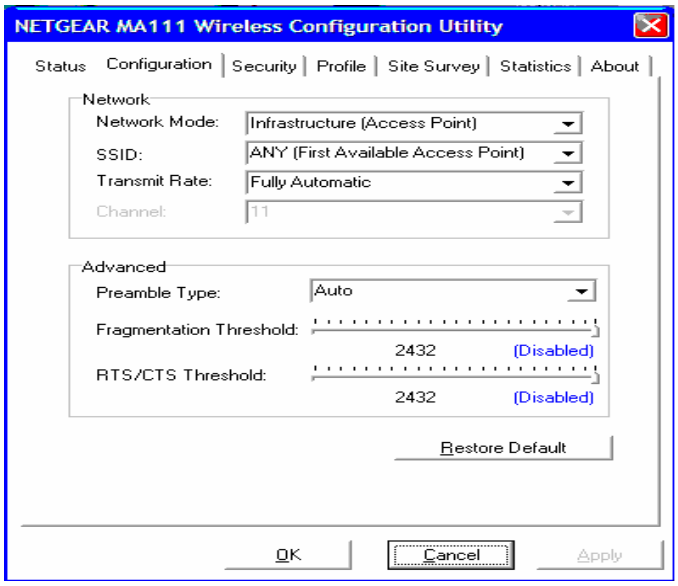
> "He goes on to say that a combination of novelty and naivety is leading to an overly- relaxed attitude toward wireless security, with many firms not even bothering to activate standard security features such as encryption. Overall, about 40 percent of the networks we sniffed out on our expedition carried some kind of encryption; the rest had been left wide open to attack."
>
> "According to IDC there are currently about 14 million wireless LANs installed around the world, a figure they expect to grow by about 60 percent over the next 12 months. Although Wired Equivalent Privacy (WEP), encryption designed specifically for wireless LANs was specified with the release of the 802.11b standard, it is notoriously breakable, and considered more of a liability than a protection."
>
> "Not only are many of the networks not encrypted, the wireless connection is placed inside the firewall, it is fairly simple to park alongside a building, log onto the network, and take advantage of their connection to download data from the Internet," Edelstein says. "Once you have the network name, you can log onto the systems and in many cases you will be able to automatically configure your device onto the network through the Dynamic Host Control Protocol."

Let's look at Netgear's MR814v2 product as an example. This product is fairly inexpensive and offers a wireless solution with little or no additional configuration. According to Netgear's MR814v2 product specifications (1998-2004), a connection can be made up to 1485 feet away from the wireless router and still have a transfer rate of 1 Mbps (Megabits per second). Better yet, one could be within to 398 feet in distance and receive 11 Mbps. There are other factors of course, such as making sure there aren't any objects that will interfere with the connection. My wireless router sits in my living room and is about 100 feet from the street. Anyone who has a wireless adapter has the capability or can at least try to hack into my network.

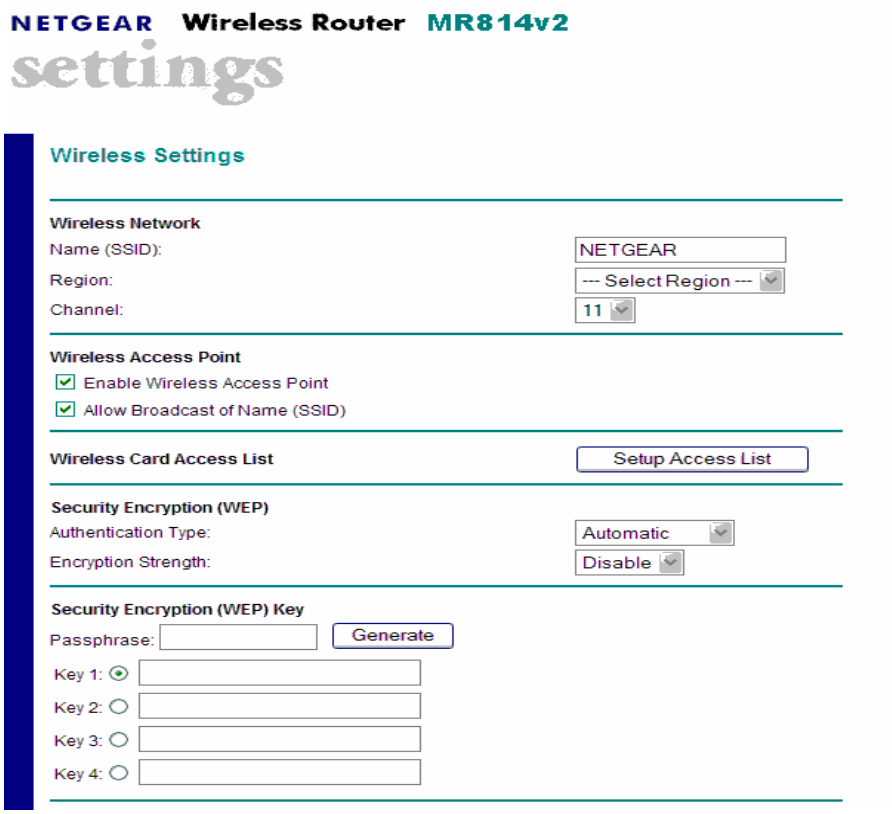
Below is a diagram illustrating this:



Looking at the picture above, if an attacker were able to guess my wireless network name (SSID-Server Set ID) he would be able to get an IP address such as 192.168.0.5. The laptop would then be on the same segment as Computer A and Computer B, which would allow probing using tools or other techniques to compromise the PC. If someone setup the wireless router and did not bother to disable the broadcast of the network name (SSID) it would be very easy to detect the SSID. In that case, the following settings on the wireless adapter would be used to detect the network name and gain access:



On the wireless router side one would see typical settings such as this:



Given the settings above it would be very easy to hack into this type of configuration. First, the SSID is NETGEAR, which would be easy to guess. Secondly, the *Allow Broadcast of Name (SSID)* is checked. The *Authentication Type* is set to automatic and the *Encryption Strength* is disabled. These four factors make this an easy wireless network to compromise.

Microsoft Critical Updates Not Applied

Microsoft has released over seven patches so far this year. It seems like every time I just get one patch rolled out another comes along. Keeping remote users up to date on these security patches is essential, especially when it comes to PCs or laptops that are connected to DSL or cable modems. These PCs or laptops are usually online longer than those connected by dialup modem (some are never disconnected), which gives hackers more time to compromise them. The BBC News World Edition (2004) states: "According to Sal Viveros, security expert with McAfee Security, many home users are not aware they should fix flaws and download patches when they are identified." The W32.Blaster.Worm is a great example of why remote PCs should be patched and kept up to date. The worm scanned the internet looking for un-patched hosts to compromise. Most users are not technically orientated people and don't go out of their way to read about technical information such as security exploits and vulnerabilities. It is up to the security professionals to educate and train the users on ways to prevent attackers from compromising PCs.

Latest Virus Updates Not Applied

Viruses are probably one of the most visible security threats in the world today. According to Symantec's online security response (2004), there were over 50 virus threats in February of 2004 alone. One of the most recent viruses, MyDoom, has caused more than 38 million dollars in economic damages thus far (Gaudin, 2004). Viruses are so dangerous because most people who know how to use a computer at least know how to use email. There are a lot of users out there who are new and don't understand the implications of their actions. They simply open the attachment because they are curious or it sounds like something they are interested in and in a matter of seconds they now have a virus on their PC. The virus could contain code that installs keystroke collection software onto the PC, which records every keystroke and is invisible to the curious user. The keystroke logger software can even take periodic screen prints, all which are not seen by the user. Once users start logging on to the VPN, the keystroke software grabs the username and password, takes a screen print, and sends it to someone on the internet. That someone now has the information needed to gain access to your company's data. Viruses are so dangerous because they can reach a lot of people very quickly!

REMEDIATION

It is nearly impossible to keep a remote PC or any PC up to date the second a new virus or security patch comes out. It is also nearly impossible to keep track of the different types of media (floppies, CDs, hard copies, flash drives, etc…) that remote users handle. Controlling who may gain access to the remote PC or laptop is also difficult. We can, however, minimize the amount of risk a company

has to take. Let's take a look at some different methods and tools that are available to aide in minimizing risk in the different areas previously discussed.

One of the first things that should be done is establishing a remote access policy and procedure (Appendix B). This will provide a number of benefits. One, it gives the users the understanding of what is expected of them when accessing company data or resources remotely. It also helps in giving the users direction on how to handle all of the risks that are involved. Providing policies and procedures also raises the level of awareness and knowledge of potential security risks. A policy should contain what is expected of the user when using either a company owned laptop/PC or their own laptop or PC. The procedure should provide users with guidance on how to handle the various risks such as proper media handling, virus updates, security updates, and also how to secure the PC so friends and relatives can't gain easy access to sensitive data. Policies and procedures should be the starting point and should be implemented before anything else.

Training should be the next item on the security project list. Users should be adequately educated and trained in all areas of security. Hands-on training should include, backing up or moving data back and forth between local PC and network, updating anti-virus software, how to do screen prints, using Microsoft's Windows Update website, procedures for media handling, and overall security awareness. I have put together some examples including a remote access policy and procedure, flowchart, and a remote access form that will aide administrators in implementing a process for risk remediation (Appendix A). I have also included a "Remote User Guide" (Appendix B) section that will walk users through securing their laptop or PC. This will give administrators a resource that they could use and put into practice right away.

Files on Remote Laptop or PC are Compromised, Lost, Stolen or Not Sanitized

Controlling who has access to a PC and how they are able to access it is very important. All users should have a user account with a password no matter if they are family or not. It is essential to establish policies and procedures that reference a technical step-by-step document on how to setup users and passwords on all of the different windows operating systems and to provide training on them. Hands-on training and easy to follow documentation greatly increase the likelihood of users actually following the policies and procedures.

Media Improperly Handled

Let's take a look at how we can minimize the risk of media falling into the wrong hands. Unfortunately, this is an extremely difficult area and there is no silver bullet to solve this problem. However, I have a few suggestions that may help in reducing the risks. Let's look at CDs, floppy disks, zip disks, and flash drives. A policy and procedure for handling media should address how the user can dispose of any media that is no longer useful or that is defective. Even though

the CD or floppy disk is defective, doesn't mean data can't be recovered from it. Such media should be destroyed by using either a degausser or a company that can properly destroy the media. Paper or hard copies would be handled in a slightly different manner with the only difference being that a degausser is not applicable. You wouldn't think there would be much risk in someone digging through the garbage for those papers, but that risk is there and can't be ignored. There is a hacker technique called, "dumpster diving," defined as looking in the trash for information that help in hacking a company's network. Useful information would include IP addresses, website addresses, passwords, and usernames. I would suggest handling paper in the same way as media and making sure there is an easy process in place to collect unwanted hard copies. I would also go one step further and provide each teleworker with a shredder. This will allow them to just shred the document as they throw it away and save them the hassle of bringing in the documents. Let's face it. If it takes time and isn't easy to do most people won't do it.

Downloading and Installing Unapproved Software

This is an area that is almost impossible to control, especially if employees are using a home PC to VPN into the company network. If this is allowed we really can't tell them they can't install software. However, we can encourage them to utilize the company's technical support staff to assist them in determining if a software package should be installed. They must be sold on the idea that by running software downloads and installs past the helpdesk they are protecting themselves from installing malicious software and thereby reducing the chances of them having to pay some consultant to rebuild their PC. If teleworkers are using company owned PCs then they should be following the company's remote access policy, which should mandate approval by technical support staff before downloading or installing any software. Users should be trained on the remote access policy and be made aware of the types of malicious software, such as spyware. They can be provided freeware tools such as Adware and Spybot S & D, which do a pretty good job in removing malicious content.

Use of Wireless Networks

Wireless networks are generally weak as we learned in the "Risks" section. They are becoming very popular, and as a result there is a big learning curve for home users and businesses when implementing a wireless network. Security for wireless networks still needs improvement. Most wireless routers don't require a lot of effort to get working, so many people forget about security. There are some basic configuration steps that need to be taken to minimize the risk of someone hacking into a wireless network. The main components of tightening security are:

Allow Broadcast of Network Name (SSID)
Network Name (SSID)

Security Encryption (WEP) key
Setup Access List

First, disable the broadcast of the SSID. This will prevent anyone from detecting the SSID. This will not, however, prevent someone from capturing it. Someone could use a sniffer and find the SSID. The SSID should be treated as if it were a password for a username. This will prevent anyone from guessing it and thus getting access to the network. Setting up Wired Equivalent Privacy (WEP) encryption is necessary and should be implemented. If possible, use 128-bit encryption and set up keys for each wireless adapter connecting to the access point. Enabling the *Setup Access List* is another important piece. The *Setup Access List* allows administrators to control which wireless adapter mac addresses are allowed to connect an access point. If the adapter is not in this list, it is not allowed to connect. Setting up these main components on a wireless network will deter 95 percent or more of all intruders.

Microsoft Critical Updates Not Applied

Let's take a look at Microsoft security patches, updates, and hotfixes. I feel that the best method of handling these updates is by using Microsoft's Windows Update website (http://v4.windowsupdate.microsoft.com/en/default.asp). Here the user can easily install the updates with, of course the help of some easy step-by-step instructions. Laptops and remote PCs are not always powered on at consistent times and not always on for a significant period of time. That makes it hard to push down or remotely update the laptop and remote PCs using products such as Microsoft's Software Update Services (SUS) or System Management Server (SMS). Therefore, establishing a set of procedures that will guide the user through the installation of updates, as well as how to report back to IT support staff with the status of the update, is critical.

Latest Virus Updates Not Applied

New viruses practically come out daily, or at least it seems that way. Two products that come to mind when thinking of anti-virus software are Network Associate's product called McAfee VirusScan Enterprise and Symantec's product called Symantec Anti-virus Enterprise. I will be referring to Network Associate's product throughout the rest of this paper. McAfee Enterprise offers great flexibility in configuring both internal and remote users. McAfee Enterprise uses a tool management tool called ePolicy Orchestrator (EPO) for organizing all PCs and servers. Create groups of PCs, laptops, and servers based on preferred strategies for keeping them up to date. For example, I would place laptops and remote PCs in a separate group because they will require different settings than internal PCs and servers that are powered on all of the time. First, configure the company owned PC/laptop on the internal network by deploying the EPO agent. The EPO agent communicates with the server to enforce certain settings. For example, make sure the user can't change any settings or disable the anti-virus

software. This will ensure that remote users will always have anti-virus protection. The remote users group should be configured to use the McAfee Enterprise server and also McAfee's HTTP website repository to receive updates. This will ensure that when the PC is off-site they will have a fallback repository (HTTP website) in which they can receive the updates. The PCs should be scheduled to update at least every three hours, if not more frequently. The "Run Missed Tasks" setting should be checked. This will ensure that if an update is attempted while that laptop is powered off, then it will run the next time the user is online. PCs owned by employees should be configured to use McAfee's FTP and HTTP repositories to receive the updates. See "Remote User Guide" (Appendix B) on how to configure McAfee for employee owned PCs.

TECHNOLOGY OVERVIEW

This section offers an overview of the different technologies involved when looking at remote VPN users and security. The intent here is to provide basic terminology and understanding of possible VPN, firewall, and desktop solutions for remote users. Obviously, I can't cover all of the possible products but I will cover a few very popular ones. The products that I will be covering are BlackICE PC Protection, Cisco Security Agent, Cisco VPN 3005 Concentrator, and the Cisco Pix 501.

BlackICE PC Protection

BlackICE PC Protection is a software package that offers protection in three different areas including Intrusion Detection System (IDS), firewall, and application protection. According to Internet Security Systems (2003), the firewall component inspects all inbound and outbound packets for suspicious activity while blocking unauthorized traffic. This does not prohibit authorized traffic from getting through. The IDS component alerts the user when it deems traffic to have malicious intent or a threat. The application component has two different pieces. One is *Communications Control,* which is designed to prevent suspicious software from running on the PC such as spyware or software that tries to send information to the internet. The other piece is *Application Control*, which is designed to control which applications are opened and also to prevent applications from opening other applications. BlackICE PC Protection costs $39.95 and is an inexpensive product that is easy to install for users and offers protection without having to buy hardware. It should be used in conjunction with anti-virus software for better overall PC protection.

Cisco Security Agent (CSA)

A similar product, but much more robust is Cisco's product called Cisco Security Agent. According to Cisco Systems (2003), this product can be scaled for any organization. This product offers server and PC protection against all malicious activity. Agents are deployed to all endpoints (PCs and servers) and maintained

through a manager component. The manager component is responsible for creating software packages, security policies, alerts, etc. Some of the main features of CSA are:

- Prevention of viruses spreading throughout the organization
- Application Protection such as web servers, SQL servers, and other self-developed applications
- Defense of "Zero Day" attacks (behavioral based technology)
- Integration with other Cisco management products such as Cisco Pix, VPN, and Cisco Secure IDS

This product does, however, require a certain level of administration depending on the size of the organization. The CSA ships with over 20 different default policies that can aide in getting an organization started. This product offers a lot of flexibility to administrators while maintaining a great endpoint security solution for the entire organization. There is a stand-alone version of the CSA product.

Cisco VPN 3005 Concentrator

This Cisco Concentrator is a VPN hardware appliance that is designed strictly for small to mid-size companies. It supports up to 100 active tunnels simultaneously. It comes with a web interface that is very easy to use. It will interface with many other VPN products such as CheckPoint, Sidewinder, and Raptor. Either the VPN software client or the VPN 3002 hardware client (see reference list for more details) can be used when connecting to the concentrator. The difference is that the VPN 3002 hardware client is an appliance that resides between the concentrator and the workstation, so there isn't a need for software on the client. This allows for any operating system to be used on the workstation. The flip side is it costs approximately $750 whereas the software client is free. The concentrator also supports Active Directory on software revision 4.0 and later. In January of 2004, Cisco released software revision 4.1 for the concentrator, which offers a product called WebVPN. Here is a summary from Cisco Systems (2004) on the WebVPN product:

> "WebVPN lets users establish a secure, remote-access VPN tunnel to a VPN 3000 Concentrator using a web browser. There is no need for either a software or hardware client (IPSec or PPTP-based). WebVPN provides easy access to a broad range of enterprise applications, including web resources, web-enabled applications, NT/Active Directory (AD) file shares (web enabled), e-mail, and other TCP-based applications from any computer connected to the Internet that can reach HTTP(S) Internet sites. WebVPN uses Secure Socket Layer (SSL) protocol and its successor, Transport Layer Security (SSL/TLS) to provide a secure connection between remote users and specific, supported internal resources at a central site. The VPN Concentrator recognizes connections that need to

be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users."

Cisco Pix 501

The Cisco Pix 501 offers a great solution for home users (see References for more details on the Pix 501). It provides a great level of security that practically works right out of the box. It can be used as both a firewall and a VPN solution. It has a web interface as well for easy configuration. It also offers an easy configuration option for establishing a tunnel session to a Cisco VPN Concentrator. Here are step-by-step instructions on how to setup the tunnel between the Pix 501 and the concentrator:

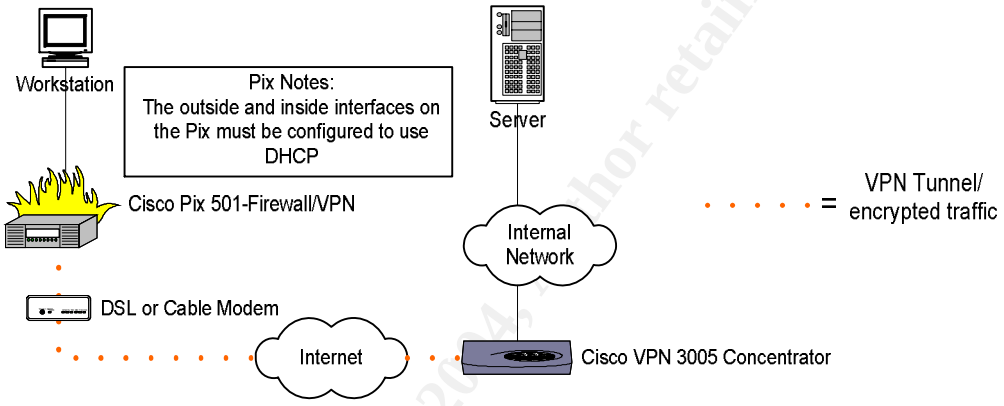
Establishing a VPN tunnel from a Cisco Pix 501 to a Cisco VPN 3005 Concentrator

Let's set up a group to allow a remote user with a Pix 501 firewall to establish a tunnel connection to a 3005 concentrator running software revision 3.6.7. We will be connecting to an NT domain in this example.

1. Connect to the VPN concentrator via the web interface.
2. Go to System|User Managemen|Groups.
3. Click Add.
4. Type in a group name called "RemoteUsers".
5. Then type in a password that is at least 10 characters which should include at least one special character, a number, and no dictionary words.
6. Then go to the general tab and fill in the appropriate DNS and WINS.
7. In the General tab in the protocols section uncheck everything except IPSEC.
8. Then click on the IPSEC tab.
9. The IPSEC SA should be ESP-3DES-MD5.
10. The Tunnel Type should be "Remote Access".
11. Authentication should be "NT Domain".
12. Under the Client Config tab make sure Tunnel Everything is selected in the Split Tunneling Policy section.
13. The default domain name should be the name of your NT domain.
14. Save your settings.
15. The next step would be to configure the Pix 501 to connect to the concentrator.
16. Connect to the Pix by opening the Cisco Pix Device Manager via Internet Explorer.
17. Then click on Configuration.
18. Then click on the VPN tab.
19. Click Easy VPN Remote.
20. Check "Enable Easy VPN Remote".
21. Select Client Mode.

22. Select Group Password in the Group Settings section.
23. Then type in the group name called RemoteUsers (same as step 3 in Cisco VPN Concentrator 3005 section above)
24. Type in password for RemoteUsers group.
25. In the Users Settings section type in a NT domain account (should be your network username you use at the office)
26. In the Easy VPN Server To Be Added section type in the concentrator public IP address and click Add.
27. Then click Apply.
28. Ping the IP address of one of your internal servers to verify tunnel connectivity.

Here is a diagram that illustrates the VPN tunnel path from the remote Cisco Pix 501 to the Cisco 3005 Concentrator:

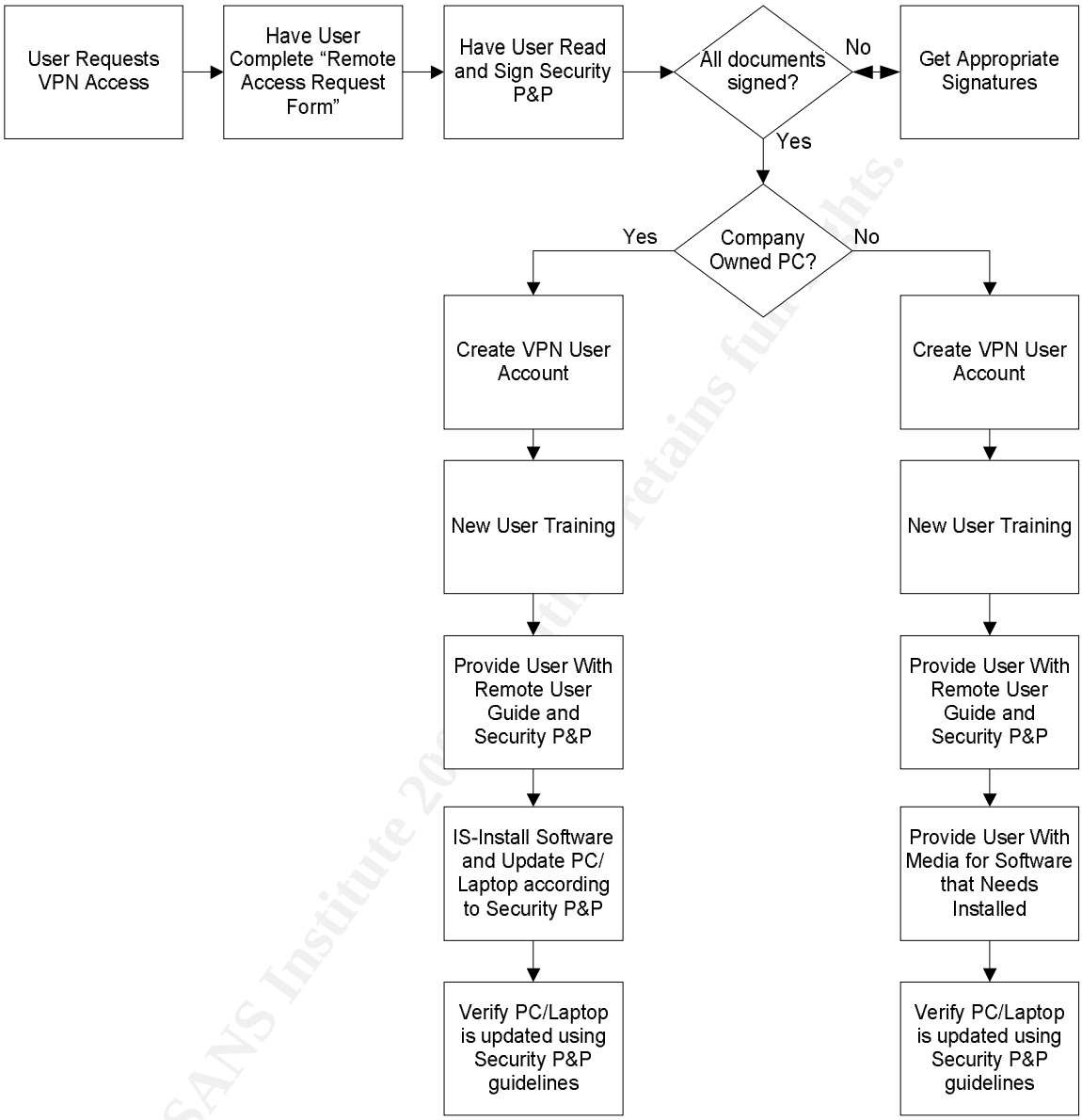


SUMMARY

There is no doubt that working from home will be a growing trend that security professionals will have to embrace and adapt to. We live in a time where malicious activity is increasing and we as professional have to increase security in order to protect the data that is vital to the company's success. We have to identify all of the risks associated with teleworkers as well as implement measures of security to reduce the number of risks and vulnerabilities. This document is intended to be a starting point and useful resource for business owners and security professionals on how to minimize the security risks when remote users connect to the company network via a VPN connection.

APPENDIX A – EXAMPLES

Remote Access Request Flowchart



Remote Access Request Form

Organization:_____
User's Name:_____
Reason for Granting Access: _____
Primary Technical Contact at Organization: _____
Technical Contact Phone: _____ Email:_____

Access Information

Check Only One:
New User: _____Change User: _____ Delete User: _____

DATA/APPLICATIONS REQUESTED
(Please check all the anticipated access needs for this user. Applications may require additional purchase of software and/or other approval.)

Check all that apply:

	Personal Drive (Home Directory)		
	Department Drive		
	Email		
	Application A		
	Application B		
	Database A		
	Database B		

Comments: _____
_____
_____
_____

Requested by (Manager/Supervisor): _____ Date: _____

Approved by (CIO): _____ Date: _____

IS Staff Only:

Completed by:_____ Date: _____

VPN Username Assigned: _____

Comments: _____
_____

Remote Access Policy and Procedure Sample

[Insert Company Name]
Date: [Insert Date]
Policy Title: Remote Access
Approved by: _____ Date: _____
Purpose:

The purpose of this policy is to protect company resources by establishing a set of guidelines for users to follow when connecting to the company internal network from remote PCs/Laptops.

Policy:

Approved users connecting to the internal network to access resources must follow guidelines stated in this policy.

Employees using their own PC to access company resources must conform to the following standards:

Employees must have some kind of virus protection software installed that will allow automatic update configuration. If employees do not have virus protection the company must purchase a license. Employees will be responsible for providing monthly status reports as described in the "Status Reporting" section in the "Remote Users Guide." In the event of a newly released virus update deemed necessary for install, employees will update PCs and provide a status report to IS staff within 24 hours of receiving notification of virus update request.

Employees must install BlackICE on their home PC or laptop. The employee must have the company purchase a license before gaining access to the company's network. Other firewall software or hardware, other than BlackICE, must be evaluated and approved by IS staff.

Employees must update PCs using Microsoft's Windows Update website to ensure PC's are patched against all of the latest vulnerabilities and exploits. They will also provide monthly status reports as described in the "Status Reporting" section in the "Remote Users Guide." In the event of a newly released patch deemed necessary for install, employees will update PCs and provide a status report to IS staff within 24 hours of receiving notification of update request.

When employees are going to dispose of the hard drive or PC/Laptop they must allow IS staff to properly sanitize disks. This will ensure that sensitive company data will not be recovered by an unauthorized person(s).

Employees must dispose of all media properly according to the instructions in the “Remote Users Guide.” Hard copies should either be shredded or brought back to the company for proper disposal. All other media such as floppies, CDs, and flash drives should be brought back to the company as well for proper disposal.
Employees should use extreme caution when downloading and installing software. It is in the best interest of the employee and the company to have IS evaluate the software in question before installation. This will not only protect the employee from accidentally installing malicious software but also protect company data.

Employees must enable usernames and passwords on their PC to ensure that only employees have access to their documents. Any other user accounts on the PC should not have administrator rights or should not have access to the employee’s profile.

Employees using a company PC/Laptop then the following standards must be followed:

IS staff will install and configure virus protection software PC before giving to employee. The employee will be responsible for providing monthly status reports according the “Status Reporting” section in the “Remote Users Guide.” In the event of a newly released virus update deemed necessary for install, employees will update PCs and provide a status report to IS staff within 24 hours of receiving notification of virus update request.

BlackICE PC Protection must be installed on every company owned PC/laptop. Therefore, employees must have the company purchase a license. Once the licensed has been received the IS staff will install the software before giving the PC/laptop to the user.

Employees must update PCs using Microsoft’s Windows Update website to ensure PCs are patched against all of the latest vulnerabilities and exploits. They will also provide monthly status reports according the Status Reporting section in the Remote Users Guide. In the event of a newly released patch deemed necessary for install, employees will update PCs and provide a status report to IS staff within 24 hours of receiving notification of update request.

IS staff will properly sanitize all PC’s according to the “PC Disposal” policy.

Employees must dispose of all media properly according to the instructions in the “Remote Users Guide.” Hard copies should be either shredded or brought back to the company for proper disposal. All other

media such as floppies, CDs, and flash drives should be brought back to the company as well for proper disposal.

Employees are not allowed to install any software without written approval from IS staff.

The procedures should be followed in accordance to the “Remote User Guide.”

Procedure:

The procedural part of this policy is deferred to the instructions found in the “Remote User Guide”.

APPENDIX B - REMOTE USER GUIDE

How to Create a Strong Password

Use the following guideline when choosing a password:

- The password should be at least 8 characters long
- The password should not contain dictionary words
- Use at least one special character (*&^%$#@!)
- Use at least one capital letter
- Use at least one number

Here is an example of a strong password: Spr!ngT!m3$
Here is an example of a weak password: SpringTime1

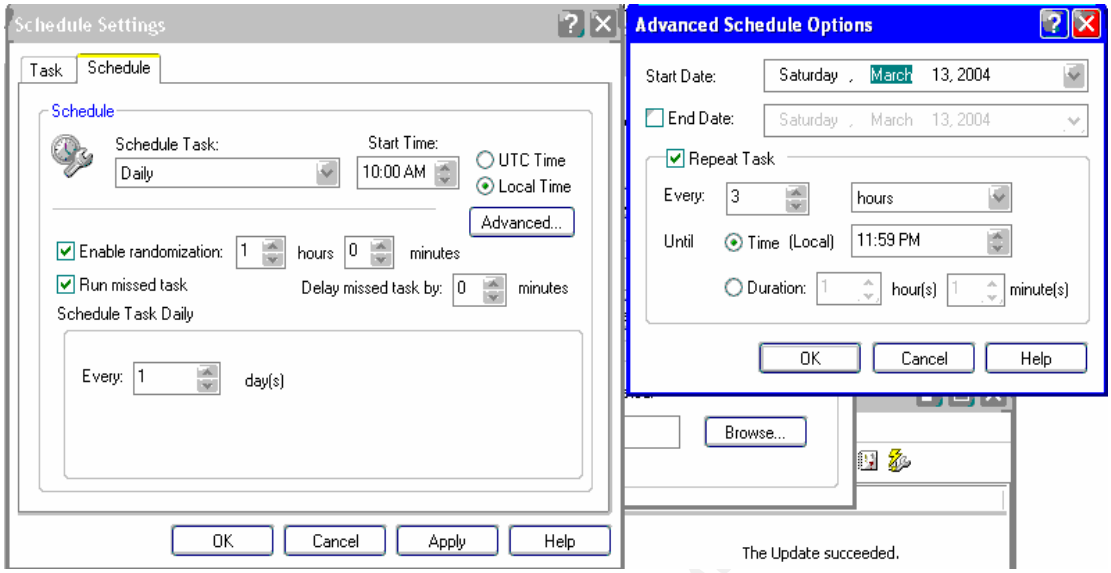
BlackICE Installation and Configuration

1) Double-click “My Computer” on the desktop.
2) Double-click bipcpsetup.exe.
3) Click Next at Welcome.. screen.
4) Click I Accept.
5) Enter Key – 141CC20-RS-34B24 and click next.
6) Accept Default Location and click next.
7) Accept Default Location and click next.
8) Click AP=Off and click next.
9) Click Next to Start Copying Files.
10) Uncheck “I would like to view the README file”.
11) Click Finish.
12) Edit BlackICE settings by right-clicking on this icon in the lower right-hand corner of your screen and select Edit BlackICE Settings.  .
13) Click the Firewall tab and set to Paranoid.
14) Then click on Packet Log tab and check “Logging Enable” and use default settings.

McAfee Anti-Virus Install and Configuration

1) Setup type: Typical
2) Click “Install.”
3) Uncheck “Update Now” and “Run On-Demand Scan”, and click “Finish.”
4) (The PC will now reboot if there was an earlier version of McAfee Antivirus installed)
5) Right-click the Vshield in the system tray and select “VirusScan Console.”
6) Right-click “On-Access Scan” and select “Properties.”
    a. General Settings: no changes
    b. All Processes: Detection → What to scan: Default + additional file types
        i. Exclusions: Add…pagefile.sys

7) Right-click “AutoUpdate” and select “Properties.”
    a. Schedule…Schedule:



8) Right-click “Email Scan” and select “Properties.”
    a. (If asked to make MS Outlook your default email program, say yes; if Outlook has not been config’d you’ll be prompted to do so)
    b. Detection → Scanning of attachments: Default + additional file types
9) Right-click “Scan All Fixed Disks” and select “Properties.”
    a. Detection → What to scan: Default + additional file types
        i. Exclusions: Add…Files protected by Windows File Protection
            a. Add…pagefile.sys
        ii. Schedule…Schedule: Weekly (every 1 week, Mon-Fri), 1:00AM, random: 2 hours
        iii. Run missed task should not be selected
10) Select “AutoUpdate” and click “Start” (the green arrow).

How to Update Virus Software

Viruses are coming out very frequently these days and it is imperative to keep up with the virus updates. Use the following instructions to update your PC to the latest virus files:

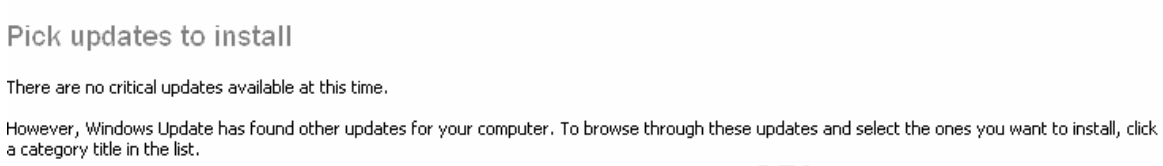
1) Right-click on the shield in the lower right-hand corner of your screen.
2) Click on Update Now.

How to use Microsoft Windows Update Service

It’s important to keep up with the latest security threats and vulnerabilities in order to prevent hackers or viruses from compromising the PC. Please follow these instructions to update your PC:

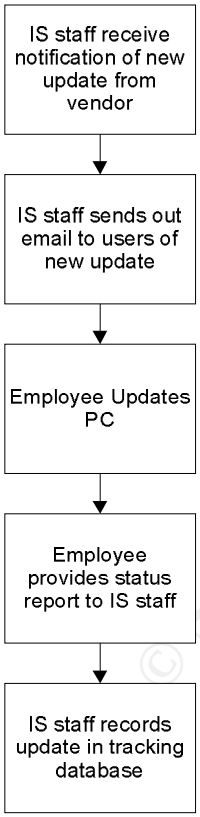
(1) Go to Microsoft’s Windows Update site by going to www.microsoft.com.

(2) In the left hand side of the web page under Resources click on Windows Update.
(3) Then click “Scan for updates” in the middle of the screen. If it doesn’t come up right away then click the refresh button until it does.
(4) Once it is finished scanning click “Review and Install” updates unless it states “There are no critical updates available at this time”.
(5) Repeat steps 3 and 4 until you receive the following message:

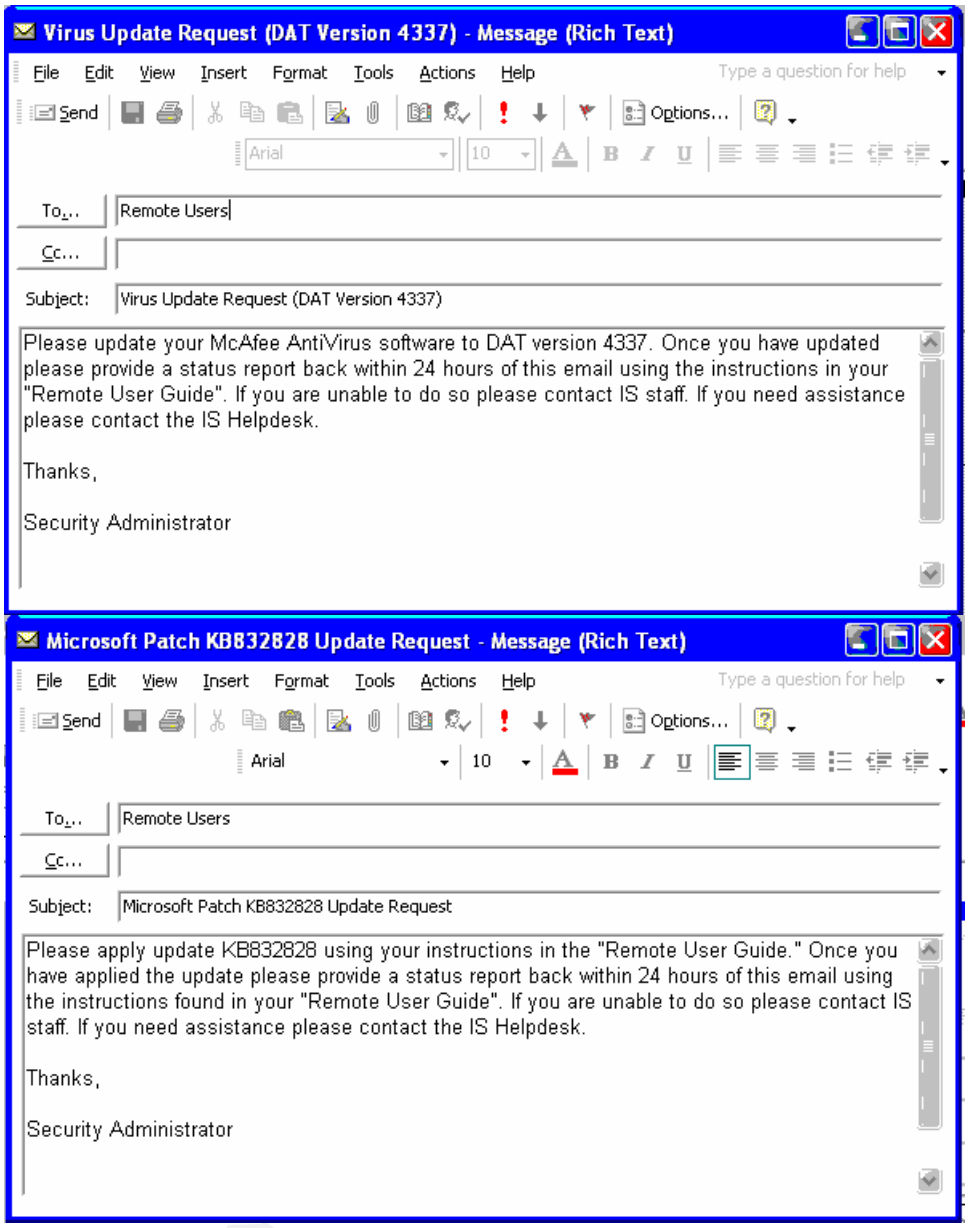


Status Reporting

It’s crucial to keep up with the Microsoft and virus updates that come out almost weekly. This section is designed to help IS in making sure that these updates are done in a timely manner. We need your help in making this happen. Below is a flowchart that describes the entire process:



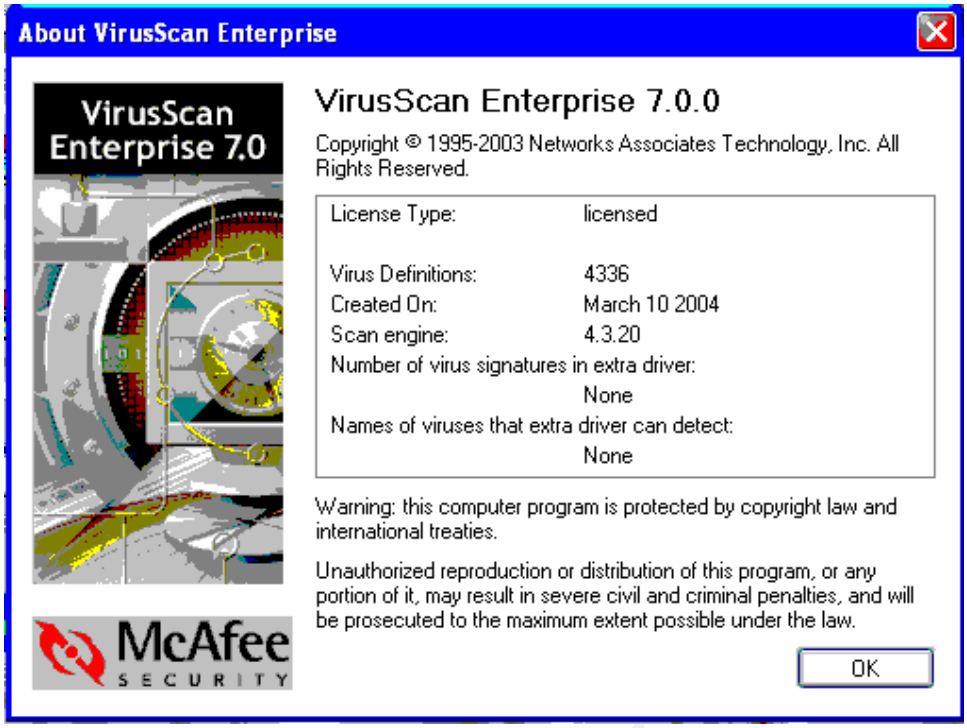
First, you will receive an email requesting you to update either your antivirus software or installing a patch from Microsoft using Windows Update Service. The emails will look something like this:



Once you have updated either the virus software or applied a Microsoft patch that was requested by IS, then follow the instructions below to provide IS with a status report:

<u>For reporting status on anti-virus updates do the following:</u>

1) Right-click on virus shield in the lower right-hand corner of your screen.
2) Then click “About ViruScan Enterprise…”
3) This is what you should see:

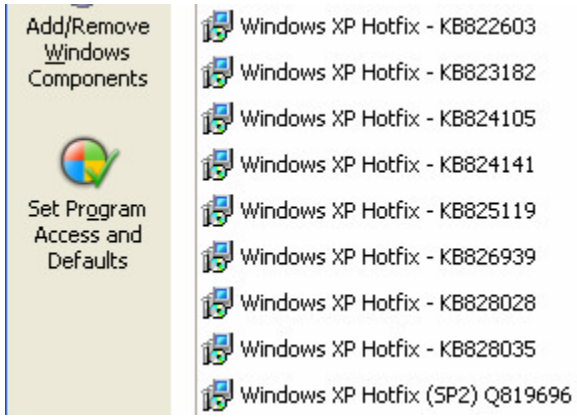


4) Then hit the print screen (prt sc) button on your PC/Laptop.
5) Open Microsoft Word or Paint (Start|Program Files|Accessories|Paint).
6) Click on the Edit menu at top of the screen and then click paste.
7) Save the file and call it virusstatus.doc or virusstatus.bmp (if Paint was used.)
8) Open up your email and attach the file you just saved in step 7.

<u>For reporting status on Microsoft updates do the following:</u>

OPTION 1:

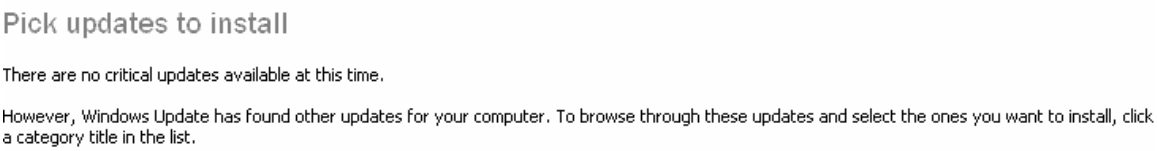
1) Go to Start|Settings|Control Panel|Add/Remove Programs.
2) Scroll until you find the update that was requested by IS to install. It should be a number either starting with a Q1111111 or KB1111111. It will look something like this:



9) Then hit the print screen (prt sc) button on your PC/Laptop.
10) Open Microsoft Word or Paint (Start|Program Files|Accessories|Paint).
11) Click on the Edit menu at top of the screen and then click paste.
12) Save the file and call it kb[number]status.doc or kb[number]status.bmp (if Paint was used.) Example: kb826939.doc or kb826939.bmp.
13) Open up your email and attach the file you just saved in step 7.

OPTION 2:

1) Go to Microsoft's Windows Update site by going to www.microsoft.com.
2) In the left hand side of the web page under Resources click on Windows Update.
3) Then click "Scan for updates" in the middle of the screen. If it doesn't come up right away then click the refresh button until it does.
4) Once it is complete you should see a message like this:



5) Then hit the print screen (prt sc) button on your PC/Laptop.
6) Open Microsoft Word or Paint (Start|Program Files|Accessories|Paint).
7) Click on the Edit menu at top of the screen and then click paste.
8) Save the file and call it kb[number]status.doc or kb[number]status.bmp (if Paint was used.) Example: kb826939.doc or kb826939.bmp.
9) Open up your email and attach the file you just saved in step 7.

If you have any problems with any of the above steps please contact the helpdesk and we will be happy to assist you.

REFERENCES

BBCi. “Protect PCs' Microsoft users told.” 11 February 2004. URL: http://news.bbc.co.uk/2/hi/technology/3477899.stm (5 Mar 2004).

Cisco Systems. “Cisco Pix 501 Security Appliance.” 1992-2004. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b18.html (15 Mar 2004).

Cisco Systems. “Cisco Security Agent Data Sheet.” 1992-2003. URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade37.pdf (16 Mar 2004).

Cisco Systems. “Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.1.” 2004. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/prod_release_note09186a00801f237a.html#76900 (17 Mar 2004).

Cisco Systems. “Understanding the VPN 3002 Hardware Client.” 1992-2004. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_getting_started_guide_chapter09186a00801f0dfe.html#1030287 (17 Mar 2004).

Douglas, Jeanne-Vida. “Wireless hacking: the art of Wardriving.” 5 June 2002. URL: http://www.zdnet.com.au/news/security/0,2000061744,20265777,00.htm (5 Mar 2004).

Gaudin, Sharon. “Mydoom Leads Damaging January Attacks.” 3 February 2004. URL: http://news.earthweb.com/stats/article.php/3307801 (8 Mar 2004).

Gaudin, Sharon. “Number of Teleworkers Skyrocketing.” 9 September 2003. URL: http://itmanagement.earthweb.com/career/article.php/3074631 (18 Feb 2004).

Internet Security Systems, Inc. “BlackICE PC Protection Getting Started Guide 3.6.” 19 February 2003. URL: http://documents.iss.net/literature/BlackICE/BIPCP-GSG36.pdf (14 Mar 2004).

LSoft Technologies. “Standard DoD 5220.22-M.” 2002. URL: http://www.killdisk.com/dod.htm (6 Mar 2004).

Mike. “Unsuspecting Computer Users Relay Spam.” 20 May 2003. URL: http://www.techdirt.com/articles/20030520/0217244.shtml (8 Mar 2004).

Miller, Ron. “Broadband Poised for Takeoff”. 29 January 2004. URL: http://www.internetnews.com/stats/article.php/3305991 (20 Feb 2004).

NETGEAR. “Wireless – 802.11b – model MR814.” 1998-2004. URL: http://www.netgear.com/products/details/MR814.php?view= (4 Mar. 2004).

Spencer, Brad. “Open relays and open proxies – your big opportunit.” 20 May 2003. URL: http://www.techdirt.com/articles/20030520/0217244.shtml (8 Mar 2004).

Symantec. “Symantec Security Response.” 2004. URL: http://securityresponse.symantec.com/ (7 Mar 2004).

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event