Global Information Assurance Certification Paper

Securing Telecommuters: Possible threats and solutions
Paul Turpin
SANS-GSEC Practical assignment
Version 1.4b option 1
July 9, 2004

Abstract:

Telecommuting is becoming increasingly more popular these days due to its leisure like advantages. Employees and employers alike are benefiting from its convenience but as always there is a downside. Vulnerabilities are abundant when work is done away from a secured office. Some of the risks associated with telecommuting include physical access to the users pc, access through the Internet, and unsecured networks to name a few. While all of these vulnerabilities are fairly easy to secure, it is very important to understand the different ways to protect against them. Insufficient resources or knowledge by the employer or employee in one area could be disastrous to the company. This paper will make you aware of the modern day threats surrounding telecommuters and how to layer your defenses to protect against them.

Threat 1: Physical Access to the users pc

The whole idea of telecommuting is to work at a different location than the office. Big companies continue to grow and office space is low so telecommuting is playing a major role in expansion. While telecommuting is a great way to deal with expansion problems, it also opens up the door to attackers by giving them the opportunity to hack into your company without having to deal with the security features of a secured office. Attacks, which could never take place in an office, are now very feasible and with new technology becoming more popular like camera phones, opening an important e-mail in a coffee shop now becomes an inherent security risk. An attacker sitting behind you can easily take pictures of your email without you even knowing they were looking.

Besides cameras, there is also a more physical threat of your computer actually being

stolen or tampered with. At home or on the road, few things stand between your personal pc and an attacker and they won't think twice about going through you or your house to get the information they need. Even people who are not attackers can compromise your computer unknowingly. Spouses and children love to download songs and games from the Internet but these actions could expose your personal data if a virus or Trojan horse is enabled.

Even human error can compromise a company's data. An employee may misplace or loose a disk or cd with important information on it, which leaves it in the hands of whomever may find it. For instance, if the cd of the company's new invention gets lost and someone else beats them to the patent, the destruction done to the company is too great to put a price on.

Deliberate acts to the users pc are also a threat. If a disgruntled employee becomes a telecommuter and has access to the company's resources outside the office, he can cause great demise to the company. He may choose to destroy the data he has by way of fire or water. He can delete or overwrite the data causing it to be lost. Or, he may make copies of the data for other purposes such as selling them to a competitor or attacker.

Threat 2: access through the Internet

Dsl and cable modems are replacing dial up modems due to their high-speed connection and reasonable costs. This is a great advantage because downloads and server access is done quicker and more efficient, but this also leads to new security risks.
The high-speed connection lets the attacker make faster probes for vulnerabilities. Also, since dsl and cable modems are always connected to the Internet, the amount of time the attacker has to hack in is unlimited. This is due to the IP address never changing if the Internet connection is not broken. It is possible to stop the connection manually but this is often overlooked due to its inconvenience.

Dial up modems are thought to be safer since they are not connected all the time and they have a different IP address every time they connect. As with dsl, an attacker would only be able to hack in when the computer was connected to the internet but since dial up connection is not feasible to be left on all the time, the time spent connected is reduced. Most of the time, hackers are looking to use you pc to relay them to something bigger like your companies network and a dial up connection would slow this down considerably. The only problem with this more secure method of Internet connection is that it's considered unpractical for business use because of its slow speed. Both methods discussed have their advantages and disadvantages as shown in the graphic below (Nahar 2).

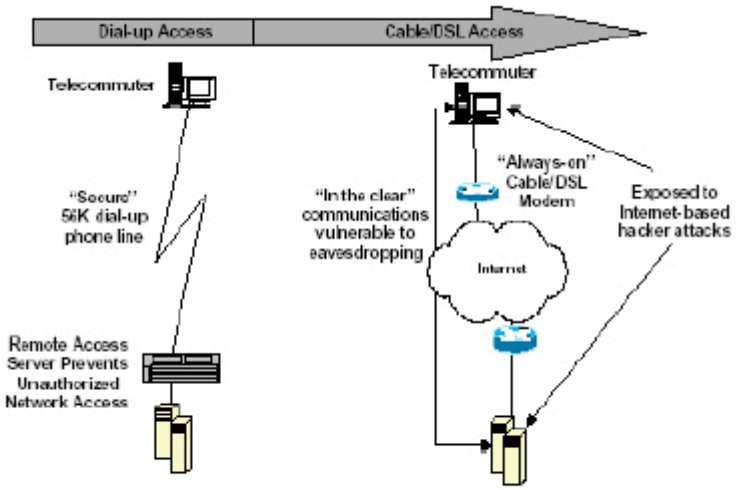


Figure 1: Broadband Access Security Challenges

Threat 3: access through the network

In order to make telecommuting as effective as working in the office, a telecommuter needs access to the same resources they would have available at the office. The easiest way for him to gain access to company's data is through their network but this also leads to more vulnerabilities. Small networks are the targets of many attackers because they can allow unlimited access to the company's databases. While it is important that the telecommuter have access to the available resources, it is just as important to be aware of the known risks associated with networking outside the office building. An attacker can use something as simple as a port scan on your network to find out valuable information in order to gain access to the corporate network.

For a cable network, wiretapping is a major risk. "On some kinds of LAN cabling, access to a LAN socket may be sufficient to eavesdrop all the network traffic on the local area network (Sicherheit)." Just think of the damage that could be done is someone had a constant watch over all of your network traffic and the worst part is, this could very easily go undetected since it is inside your firewall and unencrypted.

Wireless networks are becoming more popular due to the fact that cables don't have to be run everywhere but they are also more susceptible to attacks. Wardriving can be used to collect valuable data about your LAN. If your LAN is not configured properly so the boundaries end where the network ends, this leaves the network wide open to anyone with software on their laptop that allows them to connect to a wireless network. Granted,

they have to be close to your house, but even your neighbors could take advantage of this and while they may not be a risk at first, if they learn what they have access too and how to use it to their advantage, it could very easily turn into a major risk.

Another risk for networks is hooking up to another pc in your home. You may use your pc for work and have it secured by a firewall but if you are networked to an unsecured family computer which is used for downloads and gaming, the risk of being infect from this computer now becomes a threat. If your computer is programmed to trust this computer and it has a virus, or is hacked into, then they just bypassed your defenses by coming in through a trusted network computer that isn't secure.

Threat 4: Viruses

The easiest targets for computer viruses are personal computers. Boot viruses, file viruses, and macro viruses are all different types of viruses the telecommuter has to be aware of. Boot viruses spread by boot disks, File viruses spread by contaminated files being opened, and macro viruses spread by files even if they are not opened. If a telecommuter's pc becomes infected with any of the above viruses and then links up with the companies network, these viruses can be spread through the whole network.

Solutions:

As you can see, the threats associated with telecommuting are great. Attackers have a wide variety of openings available to them to compromise your company's resources. These attacks can range from an attacker actually stealing your laptop out of your home, to using techniques such as wardriving to tap into your wireless LAN. While it seems like there are a lot of ways to be taken advantage of, there are even more ways to protect yourself. Using these security preventions in conjunction with each other and taking a proactive role will greatly reduce the threats associated with telecommuting. Defense in depth is the best way to fight telecommuting attackers.

Solution 1: Protecting the users pc

Earlier we discussed the threats associated with your pc, now its time to discuss the many ways to protect it. We already know that pc's are more vulnerable outside the office so it is very important use security in layers to make sure it and all the information on it is protected

Some of the physical ways of protecting your pc include using strong cables and straps to anchor the computer to a heavy item, which prevents it from being stolen. There are alarms available that will alert you if someone tries to get into your computer case. There

is even software available that will signal you when your stolen pc is connected to the Internet so you can track it. Using any of these devices will help protect your pc from theft.

It is also important to use common sense any time you are telecommuting. With the example I gave earlier about camera phones, just think about the risks and it is easy to eliminate them. Sit with your back to a wall and no one will be able to get behind you to get a picture. Some other rules that should be followed are:

- Never leave your computer alone, even if just for a few seconds. Attackers don't hesitate to take advantage of every opportunity that arises.
- Try to pick a computer case that doesn't make it obvious about what you are carrying. Don't make it any easier to tell that you are toting expensive hardware.
- Mark your computer in a way so that if it is stolen, it can easily be identified. This marking should not be able to see very easily so they can't change it or take it off.
- Don't let any unauthorized user access your pc. This includes kids and spouses. Make it extremely clear to them that your pc is to be used by you and for your work only.
- Stay organized! This is a simple step to ensuring that you don't loose or misplace any information that may be valuable.
- Try to store all of your valuable information directly to the pc so you don't run the risk of having a disk stolen.

Encryption is another good layer of defense for the personal pc. One guideline to use when selecting an encryption component is that "Encrypted algorithms used by government agencies should be approved by the BSI. Outside government agencies, the DES is suitable for medium security requirements, while the triple DES is suitable for high security requirements (Sicherheit)." In making sure that all data is encrypted when not in use, it ensures that it is safe. Documents and other important information may be stolen but it does no good to the attacker if it is encrypted. Data should also be encrypted any time it is exposed to the Internet. Data being sent to and from the corporate network needs to be encrypted so that anyone who sees the data, whether intentionally through a sniffer, or unintentionally due to the wrong address, cannot read it. Some of the devices talked about later in the paper will encrypt data automatically for you.

Identification and authentication are a must for a pc. Here are a few guidelines to follow for strong identification and authentication.

- Passwords and other important information must be stored encrypted
- Access mechanisms are in place and are programmed so the computer does not allow brute force attacks to crack the passwords.
- Passwords should be a minimum of 8 characters, not all letters, and should be changed often.
- If the pc is inactive for a certain amount of time, it will go dormant and can only

be reactivated by reentering the password.

Logging mechanisms are another good defense technique. They document all the information the user on the computer has done. This is very useful for catching and tracing attackers. Some things that should be logged include the user id, date, time, what was done, and any errors that occurred. These logs should then be encrypted and stored in a restricted area so that an attacker can't cover his entrance up. The program should also be set so that it cannot be turned off. Regular checks of the logs should be done to ensure that no unauthorized user has gained access to the pc. Many logging programs can be set to automatically report any security breeches.

Anti virus software is another key part of your layered defense. "Programs which scan IT systems for known viruses have proven to be the most effective means of combating viruses(Sicherheit)." This is due to the fact that if kept up to date, they detect all new and old viruses before they take over your machine. Keeping the program up to date is key because new viruses are created daily and it is important that it scans your computer for all viruses, even brand new ones. These programs can be set to scan on a regular basis and only files that you want scanned. Resident mode is also a good mode to have your virus scanner on. This means "…the virus scanning program is loaded into the main memory when the computer is started, and remains active until the computer is switched off (Sicherheit)". This seems to be the most effective way to ward off viruses.
Also, make sure to scan any new programs you get either off the Internet or from software. These are easily overlooked but may often hold viruses.

Solution 2: Protecting company assets from the Internet

One way of protecting yourself from the Internet is to not be on it all the time. When no one is using the pc, disconnect the computer from the Internet either by an option on the computer or by unplugging it. Obviously an attacker can't break into a computer if he has no means of getting in. Also, by disconnecting every time, your pc gets a new IP address so it is harder for the attacker to find your specific computer the next time you log on.

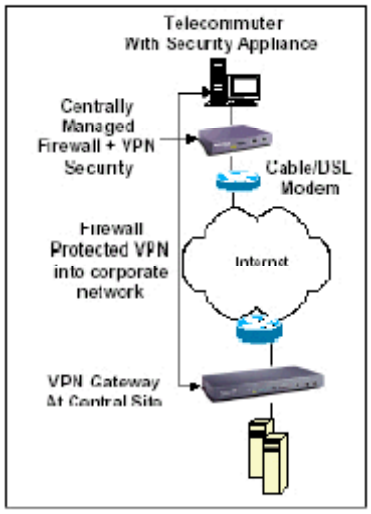
Another way to protect your computer from the Internet is by changing the computers settings. Simple changes such as uninstalling client for Microsoft networks drastically reduce the security threat to your pc. Also make sure your computer is up to date on hot fixes so that any known vulnerabilities will be fixed.

Virtual Private Networks (VPN's) are the most popular method of connecting telecommuters and their companies and for good reason. VPN's are cost effective because they use a public network like the Internet to connect the telecommuter to the companies network. . VPN's can be configured from the network components you already have in place like your OS, but the best method for implementing a VPN would

be to install a specific device for this purpose. Cisco and Multitech are two companies that have firewalls available with VPN capabilities. While this may prove to be more expensive than working with what you already have, it is worth it to keep the network functioning properly. Once the hardware or software is installed, all it takes is time to configure the VPN right and a mode of secure communication is obtained. Configuring your VPN will be different according to what programs you are using so a little research on the internet will be required to get the right setup. VPN's mostly use encryption to secure the information that is being transferred. The information leaves in "cleartext" form, is transferred into "ciphertext" as it travels the Internet, and then is returned to "cleartext" when it reaches its destination. While this method is very successful in keeping your assets confidential, this is not the only method of security that should be used. Firewalls should be used in conjunction with your VPN to ensure that an attacker cannot get into the companies network through your VPN.

When Telecommuting a firewall is a must. Whether it is a stand-alone firewall that is situated outside your network or a software firewall that is inside your network, either one will do the trick. A hardware firewall is probably more feasible for the company at the actual network. For the telecommuter, a software firewall would be enough. The firewalls purpose is to protect your pc from the Internet but in order to do this there are some features that a good firewall must have. A logging device is a must. This will tell you what unwanted packets are trying to come in or go out of your network and where they are coming from. This will help assist you in finding out if your pc is compromised. Another feature the firewall should have is the ability to hide your port so that unauthorized entry does not occur. Automatic lockout is another good feature that simply disables your connection to the internet when it is not in use so it lowers the amount of time attackers have to try to compromise your ip address. Connection notification is in place to detect spyware by alerting you any time information is trying to leave your pc. . Some basic guidelines to follow when configuring a firewall is to shut off any ports that are not being used, enable stealth mode so that your computer seems invisible on the Internet, and also enable all the features that were talked about earlier. Just like with the VPN, every firewall should be configured according to the situation. The Internet is also very helpful with firewall configuration

. The diagram below shows a secure VPN access to the corporate network. (Nahar 5)



Authenticity of data must also be kept. It is very important that the information that travels between the telecommuter and the company be legitimate. In order for this to be true all the time, information that is passes between the two must be checked to make sure the source of the data is correct and that the data is the original data sent from that source. This will eliminate the risk of getting false data or receiving data from the wrong source.

Solution 3: Security policy

A good security policy that covers every aspect of security in depth is a must to having successful telecommuters. A security policy is a good guideline for the telecommuter to follow in order to keep the companies assets secure. If the policy is not specific and is not enforced, then the company is at great risk of exposure. Some of the topics to cover in your security policy include:

- What employee's will be allowed to telecommunicate and how often they are required to come in to the office
- What equipment is required to telecommunicate and the restrictions on who is allowed to use this equipment. Also, that the equipment must be used for business only.
- Guidelines for physically securing your pc and your LAN
- What the consequences will be applied for lost or stolen data that belongs to the company
- What the telecommuter should do if a security breech is found
- How to set up a secure LAN or VPN
- There should be strict guidelines set forth about password length, required encryption of data, and data backup plans

- Protection from a firewall should be required
- Protection and regular updates of antivirus software should be required
- It should also state that regular checks of the telecommuter's pc would be done to ensure the companies safety.

Security policies are only as good as they are carried out to be. If the security policy covers each vulnerability in detail, but the telecommuter doesn't follow it, then it does absolutely no good at all. Frequent checks on whether the telecommuter is following the security policy are a must and to be efficient, these checks should be done at the place the telecommuter operates from. Strict penalties should also be enforced if the policy is not followed. Ensuring that policy is followed and penalizing those who don't abide by it will greatly increase your security.

Solution 4: Data Backup

One last defense layer is data backup. It is important to always make backup copies of all your work just in case something happens. Data backup programs are available and are user friendly. It only takes a small amount of time to backup your information but it will help out a lot if there is a breech in security. In order to have good backup data, a plan must be made and followed. Some things to keep in mind when developing a backup plan include

- How the data will be stored
- How often the data must be saved
- How to properly mark the data with the time and date
- How long backup data will be kept
- Which files must be copied
- How to correctly save the data
- What type of media is used to store the data
- How to properly destroy data when it is outdated

To make sure all these guidelines are followed, it is important to implement frequent checks of the backup data. These checks are important to make sure the data is good enough to be used to restore the systems to normal in case of an emergency.

Solution 5: Educating the telecommuter

Telecommuters must be warned of all the security issues related to working at home. They must be trained to watch for these risks, protect against these risks, and also react if security is broken. Some of the things telecommuters should be trained on include:

- Why security measure are so important when telecommuting. Many employees

may not be aware of the security risks involved with telecommuting because they don't have to deal with them while working in an office.

- If the data they are dealing with is very important, tell them. This will help drive home the importance of keeping it safe.
- They should be adequately trained on all the appropriate security measures discussed in this paper. Everything from the importance of having a firewall, to setting up a firewall, to keeping it up to date. Every detail is important because the more the telecommuter knows how to do, the safer the companies resources are.
- How to stay organized, motivated, and efficient. These three things are the keys to making a good and safe telecommuter.
- Ideas should be given on how to think of good passwords
- What to do in case a virus or attacker gets into the system. How to stop the attack, fix the vulnerability, and restore the system back to working order.

Telecommuters must constantly be reminded that it is a lot more dangerous working from home than in the office. Many do no realize this or if they do, they take it lightly. The more you bring this fact up, the more likely they are to take it serious and make the adjustment to being a pro active telecommuter.

Conclusion

In closing I hope that I have made aware the many present day risks associated with telecommuting. Telecommuting, while relatively new, is becoming more and more popular each day and it is important to keep up on the security measure needed to make it secure. Simple tasks such as changing your computers settings and installing an antivirus program can go a long way when used together. Any of the security measures mentioned above can be broken very easily but by layering your defense, they prove to be a strong wall against attackers.

References:

Analyzing Security Vulnerabilities 2004 CramSession June 8 2004
http://www.cramsession.com/articles/files/analyzing-security-vulner-9162003-1335.asp

DSL Brings High Speeds and Security Issues 2004 Jim Thompson Jupitermedia Corporation June 6 2004
http://www.isp-planet.com/technology/dsl_security.html

How to set up a VPN at home 2004 Ron Nutter NetworkWorldFusion April 26 2004
http://www.nwfusion.com/columnists/2004/0426nutter.html

Lock IT Down: Create Security Policies to address telecommuting trouble spots April

2003 Deb Shinder Tech Republic June 6 2004
http://techrepublic.com.com/5100-6313-5034662.html

Manually Configuring Windows Firewall in Windows XP Service Pack 2 Joseph Davies Microsoft TechNet February 16 2004
http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx

Securing Remote Access Connections May 2003 Deb Shinder Windowsecurity.com June 5 2004
http://www.windowsecurity.com/articles/Securing_Remote_Access_Connections.html

Securing the Broadband Network August 01 Sushilkumar Nahar Wipro Infortech June 5 2004
http://www.wipro.co.in/whitepaper/securingthebroadbandnetwork.pdf

Security Threats To the 802.11 Wireless Network May 2003 Jeffrey Isherwood CyberScience Lab Report June 7 2004
http://www.nlectc.org/pdffiles/security_threats_to_802.11_networks.pdf

Shields Up 2003 Gibson Research Corporation June 5 2004
http://grc.com/su-fixit.htm

Telecommuting : October 2003 Bundesamt für Sicherheit in der Informationstechnik June 5 2004
http://www.bsi.de/gshb/english/module/09003.html

Threats in Networks March 2003 Charles and Shari Pfleeger InformIT June 6 2004
http://www.informit.com/articles/article.asp?p=31339&seqNum=2

10 Tips For Mobile Security January 2003 Michael Clarkin June 4 2004
http://www.comnews.com/stories/articles/c0103wireless.htm

How to set up a VPN at home 2004 Ron Nutter NetworkWorldFusion April 26 2004
http://www.nwfusion.com/columnists/2004/0426nutter.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event