Global Information Assurance Certification Paper

Defending the VPN, BY: Matthew Mitchell

Two of the growing management issues relating to IT (Information Systems) management are the growing number of employees telecommunicating to work and the demand to secure all information systems from unauthorized access. Two contributing reasons for these issues is the increase in the number of companies establishing remote access mechanism using permanent hi-bandwidth connections to the Internet and the decreasing cost of broadband Internet access to the residence. Adding remote access to company's networks gives offsite employees' access to information, network resources, email, and the Internet. The number of telecommuters reached 6.8 million according to Infobeads, a research subsidiary of Ziff-Davis Corporation.[i] Securing the company's computers will protect the integrity, confidentiality, and availability of the data and applications that are stored on these computers. The number of internal and external malicious attacks on company's networks has increased almost exponentially due to the increase in the number of companies having dedicated access to the Internet.

Traditionally companies offered limited access to their information technology access regardless of geographic location by utilizing modems and telephone systems to dial directly in to the company's network. These dial-up connections were exceedingly expensive and required enormous amounts of maintenance by the network administrators. In addition to requiring large amounts of maintenance, these dial-up remote access solutions did not include robust security mechanisms. The majority of dial-up remote access solutions provided at most a two-factor authentication consisting of a username and password. There were no mechanisms designed to protect the integrity and the availability of the data while in transit to the RAS (Remote Access Server) and back to the client, but it is a private connection to between the client and the RAS. The introduction of VPNs (Virtual Private Networks) reduced the costs of traditional dial-up access, decreased the amount of maintenance, increased flexibility, and provided a mechanism to secure the data while in transit.

A VPN is a network connection that utilizes client-server architecture to connect the remote employee to the company's network that utilizes the Internet for transmitting and receiving data. A VPN works by a remote employee connects to the Internet via a local ISP (Internet Service Provider), a TCP-IP connection is made to a VPN server over the Internet, the client is authenticated, and all data that is transmitted and received across the Internet is encrypted. Encapsulating the data within the IP packet encrypts the data. Figure 1 displays the VPN encapsulation process.

Many organizations that have implemented a VPN-based remote access solution feel confident that VPNs provide all of the necessary security for remote users to connect to the company's network because the user is authenticated using various methods and that all data is encrypted while in transit. John Carnes, manager of information technology for HAHT Software states: "The home box connected to the Internet running a VPN to a secure corporate network is a major weakness."[ii] of protection when the method for connecting to the VPN server, the operating systems used by remote users, and the numbers of attacks originating from the Internet are closely examined. It is a fact that the majority of the employees that utilize remote access solutions to connect to corporate offices use Microsoft Windows based operating systems, both using company laptops and home personal computers. It is agreed upon in the information security

community that Microsoft Windows 95, 98, NT, and 2000 default installation is insecure and vulnerable to various attacks. The most exploitable vulnerability exists because Windows platforms use NetBIOS to communicate and share resources.

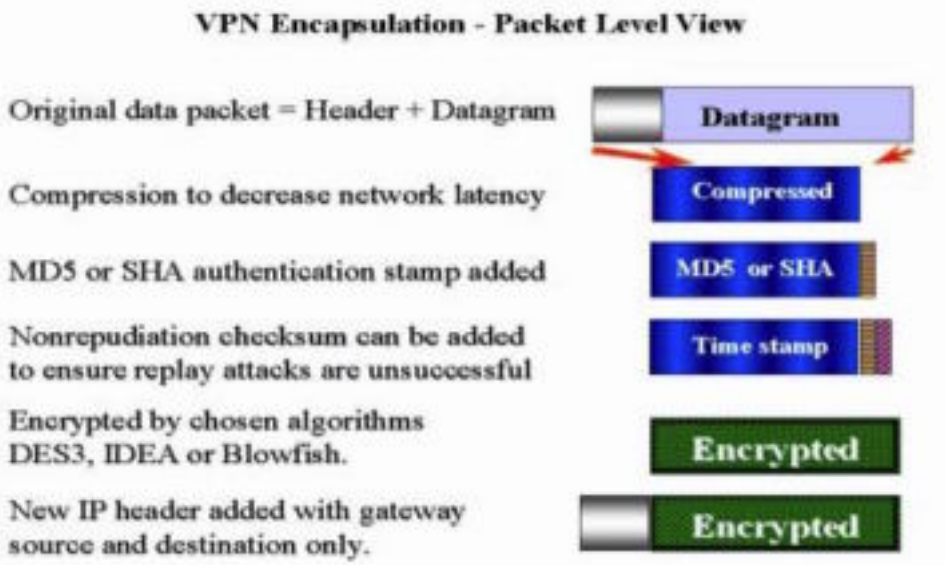

Figure 1: VPN Encapsulation[iii]

When users connect to the Internet through their local ISP and then establish a connection to the VPN server very few think about what services are listening. Most individuals do not realize that when they have established a VPN with the corporate network they are still vulnerable to attack from any individual on the Internet. The services that the user had running on their laptop while in the office, the services used by Windows operating systems for communication and sharing resources, and any other network services are still listening for a connections. The only difference from being in the office and out of the office is that the security provided by the company's network architecture is no longer there. The VPN only provides data encryption between the client and the server. Essentially the remote user's computer is extremely vulnerable to attack from the Internet and they have an encrypted backdoor into the company via the established VPN connection. Having insecure remote users connecting to the secure corporate network is a very serious security risk to the company and should be mitigated

Windows based operating systems use TCP/IP ports 135,137,138, and 139 for various NetBIOS services. These services, by default, are always listening for requests. These ports allow unauthorized access to your machine. By default the registry will allow a remote connection by any user. Information can be gathered about users, shared resources, the domain, connections, and many others. One example is if the client connected to the company using VPN technology accesses a shared network drive at the company. The data is encrypted between the client and the office, but the Microsoft network services are still listening to other requests coming from the Internet. If the network share is unprotected than any user on the Internet can connect to the client and freely access the network drive at the company without any restrictions. These are just a few of the vulnerabilities associated with Windows based operating systems and much more information is available on the Internet. The bottom line is that the vulnerabilities associated with Windows can lead to unauthorized disclosure of proprietary data,

destruction of data, insertion of malicious code, and lead to hardware or software failure. These services along with any other services that might accept any connections from the Internet should be stopped and/or incoming requests for these services should be dropped.

DSL and Cable modem access to the Internet is becoming increasingly popular among telecommuters. These connections offer a permanent connection to the Internet at broadband speeds. These broadband connections can increase the productivity of the users but it does have some level of risk. The "always on" access makes the users life a little easier but there is a flip side to this. In a recent issue of Information Security magazine published by TruSecure Labs, Howard A. Schmidt (corporate security officer at Microsoft Corporation) said the following:

"While the user benefits from the high speed and productivity, the full time connection makes them an inviting target for crackers. For instance, insecure broadband-connected machines can be taken over and used as "zombies" in a distributed denial-of-service (DDoS) attack without the user's knowledge. Worse, they can be exploited as a launch pad for a targeted attack on the corporate network"[iv]

The problem is that the computer is always on the Internet without any security mechanism in place to protect it. A telecommuter may perform all of his work during the day without event, but at night the computer may be compromised by an attacker, resulting in damage or possibly the insertion of a Trojan horse. By day the telecommuter may connect to the company network via a VPN connection and not even realize that a malicious program is running that may be designed to cause damage to the corporate network. Essentially it is similar to taking a computer that is connected directly to the LAN and moving it out on to the Internet, without any protection except for the data is encrypted between the computer and the VPN server.

The connection between the remote client on the Internet and the corporate network creates a possible transport vehicle for malicious code. Just as a user connected to the corporate LAN can be infected by a virus if preventative steps are not taken. The client computer is more susceptible to virus infection because it is now connected to the Internet without any security protection. This vulnerability needs to be addressed in order to protect the user's computer along with the corporate network.

Traditionally users that required having remote access to corporate networks have been traveling sales representatives, off-site employees, or other non-technical staff. The knowledge level, in respect to network security, of these employees is minimal at best. All these users want to do is connect to the Internet to either get access to data on the corporate network or o retrieve email. These users are usually not familiar with vulnerabilities of specific applications or operating systems. They would not know to identify an attack, nor respond to an attack. In order to protect the individuals data and the company's data steps have to be taken; either to secure the systems adequately before given to users or educate the users about network security.

In order to protect systems that are connected to corporate networks via a VPN over the Internet several steps must be taken. The previous paragraphs described different problems, which could damage the remote client's computer as well as the resources on the corporate network. Following are seven steps that should be taken to ensure that enabling remote users to establish VPNs over the Internet would not add vulnerabilities to the corporate network security posture.

Step 1: Secure the Operating System

The majority of all operating systems used by remote users are Microsoft Windows based. The default installation of Microsoft Windows operating systems, particularly Windows NT are configured with minimal or no security. After a default installation all of the latest service packs and post service pack updates should be applied. Next, all of the unnecessary services should be shut down. The following areas of the operating system should be secured: the registry, the file system, and the user account policies. Ensure that auditing is enabled. If possible only let the user who will be using this machine logon using non-administrative privileges. This will ensure that the administrator can only perform additional software installations, network configuration changes, and other changes made to the operating system. There are many different guides to securing windows available on the Internet, which will aid in this process. Microsoft has a free tool called the Security Configuration Manager that is available for free from Microsoft's website which will help expedite this process.

Step 2: Install Anti-Virus Software

Anti-virus software is not new to the security world but its value is still great. Having a quality anti-virus software package configured correctly will ensure that the known viruses in the wild will be detected and eliminated. It is very important that the software be installed correctly and updated automatically at specified intervals in order to stay up to date. If the operating system incorporates DAC (Discretionary Access Controls) the program should be configured to retrieve updates from the vendor automatically, scan the hard drives at regular intervals, continually protect the computer, and most importantly not let the user modify these configurations or turn off the software.

Step 3: Install File Encryption Software

For the remote user the immediate security concern should be what is stored on their computer. Is this data proprietary or a trade secret? What could happen if the confidentiality or integrity of this data is compromised? For these concerns encryption software should be installed on the computer and all sensitive data should be encrypted. Encrypting this data with a robust encryption standard using keys above 1024 bits will render this data useless if compromised.

Step 4: Install a Personal Firewall

The installation of a firewall is commonly the first step taken to protect a network from attacks that originate from external sources. The most common place in which a firewall is installed is after a router, which provides a gateway functionality to the Internet. Firewalls are most commonly found only inside the corporate network. If a remote user establishes a VPN connection by connecting to the Internet first, the direct connection to the Internet needs the same protection that enterprise firewalls provide. A personal firewall should be installed on the computer and securely configured. Personal firewalls are capable of providing packet filtering, block TCP or UDP ports, and possibly perform some network intrusion detection. Various vendors offer personal firewalls that are not

exceedingly expensive, are simple to install, easy to configure, and maintenance is minimal.

Step 5: Install a Host Based Intrusion Detection System

When a remote host is directly connected to the Internet they are a potential target for an attacker. As previously stated, most of the users knowledge level of information security is very low. Therefore most of these users would have no idea if their computer is under attack or if their system has been compromised. The installation of a host based IDS (Intrusion Detection System) will monitor the current configuration of the computer and notify the user or corporate network if an attack has been identified.

Step 6: Incorporate Additional Authentication Requirements

The traditional VPN or dial-up connection to a corporate network is authenticated using a combination of a username and a password. For additional security and non-repudiation reasons additional authentication mechanisms should be in place. This will decrease the likelihood of an attacker compromising the remote user's computer and connecting to the corporate network. Additional authentication can be accomplished through various methods: one-time passwords, biometrics, digital certificates, tokens, etc. These additional methods of authentication will ensure that only the specific individual using a specific computer are accessing any network resources.

Step 7: Install a Network Based Intrusion Detection System

Establishing a VPN between the remote user and the corporate network provides confidentiality by encrypting the data being transmitted and received. Commonly the VPN is terminated and data is encrypted at the firewall or after the firewall. If the remote user's computer initiated an attack, by mistake or because the system was compromised, this data will be encrypted and tunneled directly into the corporate network. To protect the corporate network from these attacks a network based IDS should be installed just after the VPN server. This will aid in protecting the internal network from attack by identifying potential attacks just after the data has been encrypted and before it is passed on into the corporate network. There are many different network based IDS products on the market. Some of these IDS look at the incoming packets and look for matches in an attack signature database; others look at the packets for abnormal behavior or anomalies. Additionally, many of these IDS products can work together with personal firewalls and other security software applications to provide central management of the entire enterprise.

These seven steps to secure the VPN are in no way a complete guide. An additional step that should be included in any corporate security policy is mandatory security training. If people do not know what can happen, what they can and cannot do, or who is liable for what than it will be nearly impossible to defend the corporate network. The bottom line is that too many companies and organizations are content with the level of security that a VPN connection provides. In order to provide a truly secure remote access solution the security must be on many levels using many security mechanisms, defense in depth. The remote user can be the weakest link in a secure network and the hackers and crackers know this. Security engineers need to provide secure solutions to this problem in order to maintain an acceptable level of risk.

[i] VPNs: Only part of the Remote Access Security Solution (Network Ice Corporation), accessed 2 November 2000, available from: http://www.NetworkIce.com; Internet.
[ii] DeJesus, Edmund X., *VPNs: Handle With Care,* Information Security, July 2000, p.48-57
[iii] VPNs: Only part of the Remote Access Security Solution (Network Ice Corporation), accessed 2 November 2000, available from: http://www.NetworkIce.com; Internet.
[iv] Schmidt, Howard A., *Securing the Home Front*, Information Security, November 2000, p. 71-73

Additional Resources:

Whitepaper: Remote Access Best Practices, Available http://www.icsalabs.net; Internet
Security for Telecommuters, Kabay, M. E., Available http://www.icsalabs.net; Internet

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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 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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event