Global Information Assurance Certification Paper

Corporate Policies for the DSL Home User

SANS
GIAC Security Essentials Certification
GSEC Practical Version 1.4b
Option #1
Submitted by: Sharon N. Mason
June 2003

Abstract

Broadband technologies have significantly enhanced the home user's access to the Internet. Connection rates at home are now rivaling those available to the corporate world. Who wants a 56Kbps dial-up when downstream link speeds up and beyond 1.5Mbps are available with a Digital Subscriber Line (DSL) connection? DSL is affordable and because it is also available in most metropolitan areas it is a viable option for the home user. However, in today's business world, where many employees access the corporate network from their home computers, the issue of how to best protect the assets of the corporate network becomes paramount. Even the best laid security practices and procedures can be compromised if specific policies for home users are not implemented, monitored and enforced.

With the increasing availability of DSL for residential services, corporations that allow remote access via traditional dial-up need to be especially diligent when establishing policies for home users. Appropriate steps must be taken to ensure that the computer an employee is using is secure and meets defined security standards. This document will focus on the issues associated with an employee that uses a DSL Internet connected home computer to dial-up the corporate network through a remote access server (RAS). It will identify the risks that exist to the corporation, stress the need for stringent security requirements and provide defense-in-depth policy-driven solutions.

Defining the Problem

With the installations of DSL technology, computers have gone from an "on-demand" mode, which requires that a connection be specifically initiated in order to connect to the Internet, to an "always on" mode, which requires the connection to be specifically "broken" in order to disconnect. To a home user, having an "always on" connection obviously has one huge benefit - there's no waiting to connect. But what happens to that connection when an employee uses that same computer to dial-up the office? If the DSL connection is not broken, you now have two "active" connections, in essence bridging a path from the Internet into your corporate network. Even if the DSL connection is broken, there are threats that still exist, for it is unknown what vulnerabilities were exploited while the computer was connected to the Internet.

The benefit of an "always on" connection to a home user translates into an even bigger benefit to the hackers of our world. Hackers don't have to wait for a connection to be established, and because the connection is persistent, the IP address of the computer remains unchanged. While threats of being attacked also exist with traditional dial-up, they are largely minimized because connection times are typically shorter in duration and new IP addresses are assigned at each connection. DSL increases the vulnerability of attack if only for the simple fact that the connection is always there and the address is seldom changed. So,

while on the surface it may appear that an "always on" connection is appealing, if not appropriately implemented, the risk to the corporation far outweighs any benefit to the employee.

Corporations spend tens of thousands of dollars on information security related products in order to ensure their networks are protected. In fact, a recent Meta Group study predicted that by the end of 2003, 55 percent of companies would be spending more than 5 percent of their budgets on security, up from 33 percent in November of 2001.[1] This obviously reflects a growing commitment to security and demonstrates that there is a significant amount of dollars being spent, but what portion, if any, of these dollars are being allocated to securing the home computers of employees? The need to secure these computers is tremendously high, for not doing so can prove to be much more costly in the long run. It only takes the exploitation of a single vulnerability on an employee's home computer to potentially mitigate all of the security measures taken to secure the corporate environment.

Employees play a critical role in defining the problem as well. Employees accessing the corporate network from home computers should not be trusted just because they are employees. It is the employees themselves who best know the systems and how the vulnerabilities can be exploited. The potential risk of attack from within is only exacerbated if an employee is terminated and adequate steps were not taken to delete their user accounts. According to Jeff Drake, the director of security strategy at IBM Tivoli, not deleting user counts is a common malpractice. He states, "We typically find that about 40% of the valid users in the enterprise are people who no longer work there".[2]

Corporations want to believe that their employees are trust-worthy and loyal. They also want to believe their employees would never intentionally damage company resources or inflict harm on the company. However, it must be recognized that most employees typically lack the skills required to secure their own computer in the office, let alone one in their home. Experience has also proven that as an employee progresses up the corporate ladder, their technical skills tend to decrease yet their access to critical corporate information tends to increase. We have all heard the saying "security is only as strong as the weakest link". Trusted employee or not, an employee working from home can represent that weak link. Acknowledging the technical capability of an employee is crucial, for it is unrealistic to expect that anyone other than a security professional will have the skills required to safeguard the corporation from the inherent vulnerabilities of the home user.

Identifying the Risks

The Webster's New World Dictionary defines risk as "the chance of injury, damage, or loss". Obviously, from a security perspective, the goal would be to remove all risk by reducing the probability of "chance" to zero. But unfortunately, when a computer is connected to the Internet, there is no way to achieve zero probability. Ignoring the risk is not an option, for in effect, ignoring a risk is

equivalent to taking a risk. Managing the risk thus becomes the most critical factor in ensuring data Confidentiality, Integrity and Availability (CIA).

Effective risk management is a strong prerequisite for establishing a successful corporate security policy. However, before a risk can be effectively managed, it must first be identified. Once a risk is identified, solutions can then be implemented to either remove the risk completely, or reduce it until it is at an acceptable level to the organization. While the intent of this document is to identify the risks that exist *to the corporation* when an employee uses a DSL Internet connected home computer to dial into the corporate network, risk management is the ultimate responsibility of each organization. Corporations must balance the risks they have identified against the goals of the organization. Only then can they implement the steps that are most appropriate for their environment.

Microsoft's web site reports there are at least 60,000 known viruses, with 95-98% of them coming through email and instant messaging.[3] The Register reports that the ratio of viruses to legitimate emails has increased from one in every 790 during the year 2000 to one in every 202 during 2002.[4] Based on this information, it is reasonable to assert that viruses and worms are a significant threat to any home computer accessing the Internet. And while installing anti-virus software to protect a computer is one of the most publicized security measures, it is quite intriguing that many home users still fail to follow this simple rule of advice. Program developers, who have been known to deactivate anti-virus software in order to improve the performance of their computers, only contribute further to the problem.

The risk of running any home computer without active *and* current anti-virus software can best be provided by examining the October 2000 Microsoft hack-in incident. As reported in an Internet Security newsletter, an employee working on a home computer opened an email attachment that set off the QAZ Trojan.[5] This in effect opened up a "back door" and allowed the intruder to have limited remote control capabilities over the infected computer.

Anti-viral vendors, aware of the worm, had already updated their software with signatures to identify the QAZ Trojan, but the scanning software on the employee's home computer was either not running or did not contain the latest updates. While Microsoft claimed none of its data was corrupted during the hack-in, they did admit to the hackers getting a look at a valuable software blueprint for a computer program under development.[6] However, since there was a known fix for the QAZ Trojan, the ramifications of the incident were far more reaching. Public perception of a successful hack-in greatly impacted the software maker's image and reputation.

This incident, while unfortunate for Microsoft, clearly demonstrates the risk in using home computers to access corporate networks. Any employee with a DSL connection at home can receive email from their Internet Service Provider or a web-based system. If they are not running current anti-virus software, their computer can become infected and when they dial-up to the office, the virus they received from the Internet can easily be propagated onto the corporate network.

The widespread impact of the Nimda and Klez worms provides historical proof that email can be a very effective delivery tool.

Exploits exist in all types of product code. However, as reported by the SANS organization, Microsoft's Internet Information Server (IIS) is number one in their top ten most commonly exploited vulnerabilities services in Windows.[7] If an employee is running IIS on their home computer, and keep in mind that a home user may not even know if IIS is running, their machine must be sufficiently patched or they are susceptible. If their home computer becomes infected, for example with the Code Red worm, internal corporate web servers running IIS can also become infected. After the Code Red worm received its notoriety in July of 2001, the majority of corporations most likely patched their Internet web servers. But did they also patch their Intranet web servers? If these machines were not patched, an employee dialing into the network can unknowingly infect these internal machines. Potentially even more dangerous, because of its dual delivery mechanism, is the Nimda worm. This worm used both email and IIS to wreak its havoc.

A hacker may not even need access to the corporate network in order to obtain access to sensitive corporate information. Many employees, after accessing the corporate network through their dial-up connection, will download the files they plan to work on to their local hard drives. Being that traditional dial-up is at best only 56Kbps, it is more cost-effective and much more efficient to work offline and then reestablish the dial-up connection to transfer the files back to the corporate LAN. The odds of this sensitive information being discovered and misused only increases if the files are not deleted from the employee's home computer after they are transferred back to the corporate LAN.

With the downloaded information existing on the hard drive of an employee's home computer, a hacker now only needs to get access to the home computer to obtain sensitive corporate information. If the hacker is intent on conducting some form of corporate espionage, they most likely may have already performed some preliminary research. A company's web site typically contains the names, and even faces of high-ranking executives. A simple search of these names at the InfoSpace web site could potentially reveal the executive's home telephone number and address. Once a hacker is armed with this knowledge, even the simplest social engineering tactics could prove effective. In fact, a ZDNet columnist, Lee Schlesinger states that "social engineering is the most serious threat to your network and your business".[8] Knowledge is power and people are more apt to disclose information to others if they believe they are talking to someone who already knows related information. Any information provided could assist a hacker in locating someone – even in cyberspace.

Certain types of internal applications can also represent another potential risk to the corporate network. Many of today's applications require client-side software or use cookies to enhance performance and collect and store application-related data. An employee, who has these applications installed on a home computer, can connect to the Internet and inadvertently make confidential information, such as user ids and passwords, available to other users of the Internet. In addition, it is also not uncommon for employees to run non-business

applications on their home computers. These applications may contain personal information about the employee. With current statistics reporting that identity theft is on the rise,[9] any personal information could potentially aid a hacker in conducting a social engineering attack on a corporation.

The actions of an employee's child must also be included in any risk assessment being performed. Children's use of the Internet can be quite varied but it is certainly not unusual for them to have their own email accounts, use instant messaging to communicate with their friends and download any music and games they can find for free. While keeping anti-virus software current is crucial, it does not provide any guarantees.

Hackers are beginning to realize that it is easier to break into someone's home computer than it is a corporate network. The perimeters of the corporate network are becoming more secure and more heavily guarded, while home computers tend to remain largely unprotected. In fact, back in July of 2001, the Cert Coordination Center already reported "a marked increase in intruders specifically targeting home users who have cable modem and DSL connections".[10] Today, it is even more critical that these "back-doors" to corporate America be securely bolted. A recent metric from the CIO web site states that more than 33 million people have broadband access in their homes.[11] As hacker techniques become more sophisticated and broadband technologies further mature, the risks will only continue to mount.

The Need for Stringent Security Requirements

Vulnerabilities are most exploited when security is lax, or lacking. It is a critical strategy to reduce the number of access points into the corporate network, but it is even more critical to know what is passing through those access points. While advancements in firewalls, email scanning and intrusion detection technology have proven to be extremely effective in the filtering and monitoring of data, this technology alone cannot protect the enterprise. In fact, the presence of this technology can actually provide a false sense of security.

Protecting the assets of an organization can best be accomplished by defining stringent security requirements that address employees accessing the corporate network from home computers. These requirements should include the use of technology wherever appropriate, but should not be so restrictive that they also significantly impact the workflow process. Risk management assessments can help to identify the security threats that exist, but it is only through clearly stated and enforceable policies, that the security goals of the organization can be successfully met.

Defense-in-Depth Policy-Driven Solutions

An employee's home computer could be classified in one of two ways: it is either an asset that the corporation owns, or it is an asset that the corporation

does not own. To control an asset, one must own it. So for a corporation to effectively manage the risks associated with an employee using a home computer to access the corporate network, the corporation needs to have control of the home computer. This is most easily achieved by having the corporation provide the computer the employee will be using from home. The provided computer would only be used for the business purpose of accessing the corporate network remotely. If the employee wanted to access the Internet via their DSL connection, or install other software for personal use, they would have to do so with another machine. However, this is no guarantee that an employee still would not misuse company-provided equipment.

Many corporations would rather not have the expense and responsibility of providing computers to employees for home use. There may also be budgetary restrictions that inhibit this practice. If the company is unable to provide the employee with a computer, then they need to determine if they can allow an employee with a DSL Internet connected computer to access the corporate network from home. Internet connectivity significantly ups the ante, and an employee may not be willing to incur the costs associated with implementing the required security measures. Even if they are, is the corporation confident that the employee can adequately configure the computer's settings? Given that The Register recently reported that human error is the most significant cause of security breaches,[12] this is clearly not a task for the inexperienced employee. The corporation must decide on the level of risk they are willing to take and the amount of resources they can allocate to the task of supporting an employee's home computer. However, it must be stressed that having control over an employee's home computer is critical in securing the assets of a corporation.

Listed below are the recommended security practices that should be employed, and included in every corporate security policy, when an employee is accessing the corporate network from a home computer:

- Anti-virus software
  The employee's home computer must be running current anti-virus software. If feasible, the corporation should license this software so that the corporation can control all administration (i.e. configuration, updates). The software should be configured so that it cannot be disabled and each time the computer dials into the corporation network, the computer should be checked to ensure it contains the latest signature files. The Symantec product, Norton Enterprise Edition is an example of software that meets this criterion.
- Operating System Patch Level
  It is critical that all appropriate patches are applied to the employee's home computer. If an automated corporate process is not available or feasible over a dial-up connection, then regularly scheduled audits must be performed on the machine and any missing updates must be immediately applied.
- Strong Authentication
  A strong method for authenticating employees from home is required in order to reduce the chance of brute force hack-in attacks. Two-factor authentication, something you have and something you know, has become a

standard practice in the industry and can be implemented with relative ease. RSA's Secure-ID is an example of a very common token-based system.

- Dial-back Technology
  This technology, which is standard on most remote access systems, can call the employee back at their home telephone number once they dial into the system. While the cost of the call is transferred to the corporation, most companies are willing to pay for the additional security it provides. Dial-back technology enhances two-factor authentication because it also requires that the employee be at a specific location.
- Encryption
  Two-factor authentication encrypts all passwords over the dial-up connection but does not encrypt session data. While it could be argued that encryption is less critical over a dial-up link than it would be over the Internet, encryption will further ensure the integrity of the data. At a minimum, data should be encrypted on the hard drive of the employee's home computer; especially if the employee will be working with highly sensitive corporate data.
- File & Print Sharing
  The employee's home computer should not have file and print sharing enabled. This is especially critical if an employee will be downloading corporate documents to their home computer.
- Services
  Any service not required should be deactivated (i.e. IIS, FTP, Telnet).
- Personal Firewall
  A personal firewall is a must if the computer will be connected to the Internet. Black Ice is an example of a commonly deployed personal firewall.
- Dynamic IP
  If the DSL provider offers the choice, dynamic IP addresses should be used over static IP addresses. The connection to the Internet should be "broken" when not in use so that each new connection receives a new IP address.
- Account Management
  The accounts for all terminated employees should be deactivated and deleted immediately. New passwords should be assigned for any system account or device that the employee may have had access to. The privileges of any employee working from home should be reviewed and if possible limited to what is minimally required for them to work from home.
- Monitoring
  Internal system and remote access log files should be reviewed regularly for any suspicious activity. The logs should be managed in such a way that they are available for historical and/or forensic purposes. If feasible, internal intrusion detection systems should be used for real-time monitoring of traffic.
- Public Information
  The home address and telephone number for top executives should be unpublished.

The above policy recommendations provide a defense-in-depth approach that, if followed, will help protect the assets of a corporation. However, it must be

noted that a corporate policy is much easier to write than it is to enforce. The enforcement of corporate policies takes time and money; resources that many corporations would prefer to allocate to other initiatives. But consistency is the key. For any corporate policy to be truly successful, it must be consistently enforced.

An employee is much more likely to adhere to a policy if the policy is clear and can be easily understood. Employees may sign a document, which states they are aware of corporate policies, but did they really take the time to read it, let alone comprehend it? One of the best complements, if not necessity, to any corporate security policy is security awareness training. Employees need to understand the importance of security and the impact the lack of security can have, not only to the organization, but also to them. Even if an employee is not accessing the corporate network from home, they most likely still have a computer at home for personal use. An employee can relate more to the simple instruction of not opening an email from an unknown source if they believe it can harm *their* asset. The trick is to make education interesting to an employee at a personal level. Any security knowledge they acquire will also benefit the corporation.

Conclusion

DSL has provided many home users with affordable and high-speed Internet access. Corporations must be cognizant of the threats that are associated with an employee using a DSL Internet connected home computer to access the corporate network and take appropriate steps to identify and minimize their risk. Allowing employees to access the corporate network remotely requires that only the most stringent security practices be implemented and enforced.

References

[1] Mullany, Darby. "IT Security Market to Double." Newsfactor Network. 29 Oct. 2002. URL: http://www.newsfactor.com/perl/story/19809.html (21 Apr. 2003)

[2] Margulius, David L. "Tackling Security Threats From Within." InfoWorld. 25 Apr. 2003. URL: http://www.infoworld.com/article/03/04/25/17FEinjob_1.html?security (28 Apr. 2003)

[3] "How Big is the Virus Problem?" Microsoft Security and Privacy for Home Users. 2 Apr. 2002. URL: http://www.microsoft.com/security/articles/antivirus.asp (2 May 2003)

[4] Leyden, John. "Home User Insecurity Spurs Email Virus Growth in 2002." The Register. 16 Dec. 2002. URL: http://www.theregister.co.uk/content/56/28585.html (2 May 2003)

[5] "Inside the Microsoft Trojan Hack." Internet Security Newsletter. Volume 5. Number 1. Fourth Quarter 2000. URL: http://www.securecomputing.com/index.cfm?sKey=616 (21 May 2003)

[6] "New Account of Microsoft Hack-in." MSNBC. 28 Oct. 2000. URL: http://zdnet.com.com/2100-11-503059.html (22 Apr. 2003)

[7] "SANS/FBI Top 20 List." SANS Institute. Version 3.23. 29 May 2003. URL: http://www.sans.org/top20/ (29 May 2003)

[8] Schlesinger, Lee. "Your Biggest Threat." Tech Update. 1 Apr. 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2859492,00.html (2 May 2003)

[9] "Identity Theft on the Rise." Wired News. 22 Jan. 2003. URL: http://www.wired.com/news/business/0,1367,57359,00.html (6 May 2003)

[10] "Cert Advisory CA-2001-20 Continuing Threats to Home Users." Cert Coordination Center. 23 Jul. 2001. URL: http://www.cert.org/advisories/CA-2001-20.html (21 Apr. 2003)

[11] "Broadband Use up 59 Percent." CIO. 17 Jan. 2003. URL: http://www2.cio.com/metrics/2003/metric489.html (21 Apr. 2003)

[12] Leyden, John. "People are the Biggest Security Risk." The Register. 19 Mar. 2003. URL: http://www.theregister.co.uk/content/55/29827.html (2 May 2003)

Last Updated: September 24th, 2017

Upcoming Training

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
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	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 Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive