Global Information Assurance Certification Paper

Lanenna T. Joiner
October 21, 2003
GIAC Security Essentials Certification (GSEC), version 1.4b

Home Sweet Home: Extended the Company Beyond the Exit

Table of Contents

Abstract

The objective of this practical is to provide a high level overview of how companies have logically gone from the physical structure of "the office" into the home-office. The shift in business introduces a new vulnerability to companies, the laptop traveling back and forth from corporate to home-office. With users spending more time at home, the company needs to be aware of all the options from connection types to security risks that could affect corporate data at home. No longer are companies just worrying about external and internal threats separately but a hybrid threat-external (attacker) and internal (employee/laptop).

Introduction

The telephone, patented by inventor Alexander Graham Bell in 1876, has continued to reach-out and touch the world through Plan Old Telephone System (POTS) in many ways. The possibility of transporting the employee from the workplace to the home; bringing them closer to their company as if the user was in the office, next to their managers, is a great accomplishment for the telephone company. Telephone companies have helped to increase the bottom-line revenue of 'Corporate America' through the extension of networks from office to office and now from office to home.

"Thanks to the combination of affordable high-speed networking and an increasingly decentralized economy, almost anyone with an understanding boss--or no boss at all--can do it."[1] Post- 911, changed the world for all. Companies in New York that suffered structural damage were forced to relocate to other buildings or telecommute from home.

There are many reasons companies are allowing users to telecommute; it could be due to a disaster, alternative work schedule, or just based in the home. And according to ABCNEWS.com, "…Bureau of Labor Statistics report released last year, more than 25 million Americans — 20.5 percent of the total workforce — reported they worked at least 49 hours a week in 1999. Eleven million of those said they worked more than 59 hours a week."[13] If users are not in the office, they are working from home. Corporate strategies should be planned and implemented based on security of the connection type combined with security of the laptops.

Types of Connections

Host Dial-Up Access

Although Host Dial-Up or Shell Account access is extremely insecure, its listed in this document as an option primarily because it is available free of charge. A few

options can be found at http://www.leftfoot.com/free-shell.html. Common application would be email (pine) and web access (lynx) both text based. As the Internet expanded, the need for more robust applications became apparent in the introduction of the Graphical User Interface (GUI). Shell Account users were not adapting to change; therefore companies were forced to make the changes for them. Lance Weatherby, executive vice president for dial-up services at EarthLink highlights, "Of EarthLink's 3.7 million users, only 2,000 had shell access." [2]

Shell Account or Host Dial-Up access is fairly simple. It "Allows a user to logon to another remote computer system, usually via modem and telephone that is itself connected to the Internet. Normally programs are run on the remote system to gain access to Internet services. Because you typically dial-up from terminal emulation software, you are restricted to text mode programs only. This means that, for example, you can only use a text-based web browser to explore the World Wide Web."[3]

Since Shell Accounts can be accessed from anywhere, Host based Access Control List (ACL) should be in place in order to specifically restricted to whom and from where your network is being accessed. Host ACLs can be used to restrict access to computers based on the company's business rules, which includes: Protocol (TCP, IP, HTTP, Telnet or FTP) and Source or Destination port. A Host Based ACLs can be written as 192.168.*.* (source IP) to 192.168.22.2 (destination IP) on port 21. Also, data including id and passwords are sent in clear text unless a secure application is used.

SLIP/PPP Dial-Up

SLIP/PPP

Serial Line Internet Protocol (SLIP) (OSI DataLink Layer) assumes error handling will be performing by upper levels in the OSI. "SLIP/PPP provides the ability to transport TCP/IP traffic over serial lines, such as dial-up telephone lines, between two computers. Both computers run some sort of TCP/IP based network software. This allows a home user to get direct Internet access from their own PC with just a simple modem and a telephone line. For many users, this is an exciting way to get direct Internet connectivity at a low cost. With SLIP/PPP, you can run your favorite GUI based web browser, ftp client, etc - right from your own PC."[3]

Point-to-Point (PPP) (OSI Physical Layer) handles error checking within its own layer. Generally, SLIP/PPP are associated because they provide the same service, but PPP is a better choice due to its error correction. Using SLIP/PPP requires the user to have their laptop modem (14.4/33k/56K) configured. "PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authenticating peer before allowing Network Layer protocols to transmit over the link."[4] SLIP/PPP authentication options are listed

least to most secure Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) and Microsoft Challenge Handshake Authentication Protocol v1 and v2. Instead of using these flawed and dated authentication method, tokens cards like RSA SecureID (although not 100% secure), should be an option. Hacker tools like Cain & Able can be used to calculate future passcodes but still requires the user's pin code in order to break into the network. Hopefully users are not taping their pins to their token cards.

To setup SLIP/PP access, users should configure Phone Dialer by accessing: Start>Accessories>Communication>Phone Dialer. The company should provide dialing parameters.

SLIP/PPP drawback is the need to simultaneous use the phone during conference calls while viewing data. For example, if the user wanted to access email, they would need to disconnect from a phone call in order to communicate with the email server. An advantage of SLIP/PPP is the option for different types of Protocol Authentication, which can be partner with a stronger authentication method, such as token cards. However, this connection type drawback is that it has a l*ower data transmission rate.*

Integrated Services Digital Network (ISDN)

With ISDN, users have the flexibility of both data and voice transmissions over the same medium, but separate channels (Send and Receive). ISDN was normally deployed in small businesses but companies began to understand the marketability of the product to home users or companies developing telecommuting strategies. "ISDN (Integrated Services Digital Network) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a modem) can see highly-graphic Web pages arriving very quickly (up to 128 Kbps)."[5] Comparatively, dial-up achieved a maximum 56 kbps throughput and ISDN was up to 128 kbps. Its decrease in popularity was due to its higher cost and complex installation compared to that of rivaling products the Cable and DSL modem.

Cable Modem

Cable Modem obvious advantages over ISDN are the cost, ease of installation and 3mbps throughput. The modem hardware contains a programmable operating system that is installed by the ISP but is also available through online auctioneers like eBay. Although companies offer modem-leasing programs, users are able to purchase a modem or lease a modem through the service provider; thus leaving the consumer vulnerable, by having to purchase computer products on the Internet through an untrustworthy site or person, presenting a serious security risk.

With the cable industry capitalizing on its existing infrastructure, it is able to offer package deals like cable television with a discount on cable modem services. To access the Internet, the cable installation requires a coaxial splitter for the cable modem wire separating cable television from the cable modem services.

A major security concern for the cable modems is file sharing. "If file sharing is enabled through NetBIOS on a Windows 95/98 computer, then it is very possible that everyone on the Internet will have read, and perhaps even write access to the shared files."[6]

Cable modem services should be combined with VPN to increase security for data sent between the user and the company. In addition, its still very likely that infected data can be introduced into the company's network.

Digital Subscriber Line (DSL)

DSL has emerged as a leader in the SOHO (Small Office Home Office) space with its affordability, data transmission rates (up to 1.5mbps) and persistent connection. **"**xDSL is similar to ISDN inasmuch as both operate over existing copper telephone lines (POTS) and both require the short runs to a central telephone office (usually less than 20,000 feet)."[7] DSL also has the benefit of static IP(s) as they may be necessary for certain applications for mainly used by support personnel.

Asynchronous DSL (aDSL) is both a analog and a digital product that allows both the computer to send/receive data and the telephone to send/receive calls through a single telephone jack. To install ADSL modems, kits are sent by service providers and include: modem, telephone wires (1 for telephone and 1 for the DSL modem), and filter. The filter functions as a barrier between digital and telephone frequencies.

Practical Steps to Securing Corporate Assets

Issue Hardened Laptops

Host hardening or configuration lock-down is the 1st level of defense. Companies should procure, test, configure and deploy laptops based on ghosted company images. Also, Microsoft's Group Policies has advantages. "Group Policies allow a security manager to set configuration details for the OS and its components …as well as other apps."[14] Having available images helps with Disaster Recovery (DR), for a catastrophic or compromising situation. "The terrorist attacks displaced some 5,000 employees at American Express' company headquarters, forcing the company to relocate most of them to other offices in Manhattan and New Jersey. But about 800 employees now telecommute, although some of those workers had telecommuted at least occasionally

before."[11] If and when a user brings a compromised laptop back into the office, users should have already copied data to a networked drive prior to leaving the office. Therefore, re-imaging the system causes minimal downtown for the user but a questionable amount of time for the company to determine the network compromise.

Anti-Virus software

Anti-Virus software defends system against viruses, trojans, and worms like Blaster. With Anti-Virus software, the client is installed on the workstation and the agent server is installed on a server setup to communicate with the Anti-Virus vendor based on pre-configurable intervals. For example, every day at 5 AM PST the corporate server polls the vendor box for updates. Updates are pushed to clients workstations from the corporate server once users login. If the user locks their workstation and does not shutdown the PC, the virus updates will not reach the clients desktop, unless the PC is restarted, leaving it vulnerable to compromises. If the PC was not updated, the user takes an outdated system home, which has an increased risk for attack. Unknown to the user or the company, the user returns to work with an infected PC.

Firewalls

Firewalls features allow applications to be configured based on IP address (source (src), destination (dst)) and ports. If an attacker is using a know signature, Back Orifice for example, the system will check its rule and could place the intruder, in the IP address deny list. The firewall application can be configured to alert the user which application or service is trying to communicate outside of the client or the corporate network. However, most users may not know how applications work nor do they ask questions about how they should work. Due to this simply pressing 'Yes' or 'OK' to bypass a pop-up is likely. With occasional office visits, home-based users may at a higher risk than other telecommuters. Developing a strategy for PC checkups in the field would be of benefit to the company. In addition, "Tying compliance to annual bonuses and promotions is a sure way to ingrain secure consciousness into the corporate culture."[15]

Virtual Private Network (VPN)

A VPN client can be installed on the laptop to create an encrypted tunnel between a user's laptop and the corporate network through dial-up or over aDSL. This tunnel allows users to transmit data safely without intruders seeing data packets that could contain sensitive information. Be mindful that in order for the intruder to intercept data, the encryption key is needed. The company may implement a stronger authentication method like a 1 time password that exists with RSA SecureID cards.

The Wireless Threat

More and more users are combining their Cable or DSL modem with Wireless products (Access Point and Wireless Card) that are making their way into the home-office. "According to Parks Associates, the number of U.S. households with a wireless home data network will swell from 3.5 million at the end of 2003 to 11 million by the end of 2007."[8] Just as the name implies, Wireless has no cables connecting the computer to the Access Point (AP). As Wireless products drops into an average consumer's price range, they are being realized as an added value.

Partner with Certified Wi-Fi Dealers

Users spend little time choosing products because of security they are focused on the price. Users knowing their company's wireless strategy or simply researching trade magazines can discover the latest wireless products available on the market. But will those same products be cost-effective in the home of a consumer? Will the chosen device be a layer in the home-office overall securities defenses or have little to no security at all?

Employees, as well as companies, that have already purchased wireless devices could greatly benefit from a guide to wireless in the home. Helpful documentation could be the difference between a poorly configured Service Set Identifiers (SSID). SSID is the network name needed by the wireless card to associate with the Access Point (AP). "The 802.11[Wireless Protocol] signal can travel surprisingly large distances from the access point, often a thousand feet or more, allowing the hackers to connect from outside the building, such as from a parking lot, or from the street, (leading to the term "drive-by hacking")."[9]

Default, out-of-box, SSIDs allow anyone war-driving or walking the neighborhood with a handheld device or laptop to associate with the user's wireless network without permission. After the offender has associated to the user's Wireless Local Area Network (WLAN), using net share from a command prompt shows hidden shares and makes gaining access to sensitive corporate data easier.

By conducting lobby trainings on some rated consumer wireless products and sharing information about the company's wireless strategy, the message of what users do at home affects the company is iterated.

Common User Mistakes—Wireless

Default SSID

SSIDs should be changed as soon as Access Point is functioning properly. Challenges may arise with home installations involving users that are unfamiliar with the technology, thus leaving the SSID unchanged is not uncommon. Not changing the SSID is just as dangerous as leaving default Windows users,

Administrator and Guest, with unchanged default passwords. A plethora of information is available on the Internet extra precaution should be taken to secure systems.

Broadcasting SSID

NetStumbler is a Windows (32-bit) application that is capable of determining SSID based on beacons that the Access Point (AP) broadcast in passive mode. (Kismet is a *nix application similar to NetStumbler operating in passive and active mode.) NetStumbler operates on a laptop or desktop only if the machine has a wireless card installed and properly configured. It captures important information: SSID, Channel (6 is default) and Filters. Even though users may not broadcast their SSIDs, NetStumbler is able to determine the SSID. Most important point captured is the Filter, which lists default SSIDs. Default settings allowing users the capability to association with the Access Points without authenticating.

Encryption

Disable, 64-bit, 128-bit Wired Equivalent Privacy (WEP) is the available algorithm to encrypt data sent from laptop to AP or AP to laptop. Take a 40-bit encryption option at the Access Point (AP) for example. "This is not strong enough encryption in today's environment. This code can be broken in a day or less by a good encryption hacker, according to University of Berkeley's research team."[10] Given a 40-bit code broken in a day and using a 156-bit for illustration it takes close to 4 days for a cracker to break the code. The lower the WEP, easier it is to crack the code.

Making an entrance into the market is the 256-bit WEP and 802.1x capable security devices. Note: 802.1x requires a Radius Server. Very few wireless cards are capable of 256-bit WEP that is available on the latest Access Points (AP). Using AirSnort, wireless cracking tool, enables a malicious user with the capability to collect between 5 and 10 million packets that increase their chances of breaking the WEP key. Encouraging users to use pass-phrases (3verYdAY!sAp!ckn!ck) instead of passwords (pumpkin) increasing the time to crack a code.

On Off Switch

Taking advantage of basic security is important as well. Utilizing the modems off capabilities when not in use is a good way to avoid cyber attacks and giving out a Dynamic Host Configuration Protocol (DHCP), IP address, to a war driver. This option exists and is configurable at the APs console. Best practice should be to limit the addresses to the number of PCs in the household.

Continuous Improvement

How-To Documentation

Create how-to documentation with instructions on how to secure data. Creating documentation to secure corporate documents empowers the user and the company. Although, encrypted documents may appear to be safe, encryption gives the user a false sense of security. If compromised, the attacker could pry deeper because of the encrypted documents.

Intruders accessing a PC with a Remote Administration Tool (RAT) similar to Back Orifice can give control to an attacker without authorization from the user. The RAT gives the attacker-unrestricted access to everything on the PC including access to change passwords, access encrypted files, and install keystroke capture tools (called key-loggers). Security by obscurity is an illusion; remember the laptop eventually returns to the office.

Peer to Peer (P2P)

Although users are finding that P2P, File Sharing and Instant Messenger (IM), privileges are restricted in the office. Their insecure home network allows users to access any website and use any restricted application like the KaZaa or similarly free applications. "Most files that are accessible using KaZaa Media Desktop originate from other users. This means that there will always be the risk of irresponsible users introducing viruses."[12]

If the company has not done anything to remove such applications from their systems or prevent future installation, users logging into their PC could unintentionally launch the P2P application. KaZaa when started goes out to contact servers that make it possible for other KaZaa users to query the PC for shared media, copyrighted material like MPEG-1 Audio Layer-3 (MP3).

Conclusion

With the home user and telecommuter community steadily growing, companies must extend their protection beyond the physical and logical borders of the company, to employees working from home. Notably recent litigation of the Recording Industry Association of America (RIAA) demonstrates the potential for companies to become entangled in litigation. Although, precedence has yet to be set in any case, companies may be found to be liable for more than users downloading music files.

References

[1] Schiffman, Betsy (July 18,2003). High Price To Pay For Working At Home.
http://www.forbes.com/2003/07/18/cx_bs_0718home.html

[2] Shankland, Stephen (July 27, 2000). Net fans bemoan EarthLink's nixing "shell" access.
http://news.com.com/2100-1023-243769.html?legacy=cnet

[3] SLIP/PPP Homepage: Access the Internet
http://sunsite.nus.edu.sg/pub/slip-ppp/access.html

[4] PPP Authentication Protocol
http://www.faqs.org/rfcs/rfc1334.html

[5] Integrates Services Digital Network (ISDN) Definition
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212399,00.html

[6] Edwards, Joe (Spring 2000). DSL and Cable Modems: The Dangers of Having a Static IP Address
http://islab.oregonstate.edu/koc/ece478/project/2000RP/E.pdf

[7] Digital Subscriber Line (DSL)
http://webopedia.com/TERM/x/xDSL.html

[8] Greengard, Samuel (Septemeber/October 2003). The Networked Home
http://business.cisco.com/prod/tree.taf%3Fasset_id=104022&MagID=103999&public_view=true&kbns=1.html

[9] Wireless Security Auditor (WSA)
http://www.research.ibm.com/gsal/wsa/

[10] Wireless LAN Security Considerations
http://www.mobileinfo.com/Wireless_LANs/security.htm

[11] Kolbasuk Mcgee, Marianne (October 22, 2003). The Home Front
http://www.informationweek.com/story/IWK20011018S0075

[12] The Guide:Security and Privacy KaZaa
http://www.KaZaa.com/us/help/virus.htm

[13] Schabner, Dean (May 1, 2003). Hard Work: Downturn or Not, Americans

Spend More Time on the Job Than Anyone
http://abcnews.go.com/sections/us/DailyNews/work_howmuch_dayone.html

[14] Heiser, Jay (October 2003). Making Policy Stick

[15] Bianco, David (October 2003). Who Do You Trust?

Last Updated: October 23rd, 2017

Upcoming Training

SANS San Diego 2017	San Diego, CA	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 Seattle 2017	Seattle, WA	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 Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
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
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
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
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 Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
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
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event