Global Information Assurance Certification Paper

Why Does My Company Care if I'm a Perv??!!
- or -
The Perilous Internet

Diane Williams
December 13, 2000

As the Waste, Fraud and Abuse coordinator for a DOE primary contractor, the unpleasant responsibility of monitoring Internet use has since 1996 fallen on my shoulders. This task entailed assisting in the production of a kajillion lines of Perl-driven C++ code to capture, crunch and ultimately report data to proper management. Being a conscious-ridden personality, when folks started losing their jobs over my reports, I lost a lot of sleep. However, this feeling soon left me as I started realizing what was coming down. One thing that made me feel better was the fact that I was working my butt off for this company and sometimes making it home in time to crawl into bed and get a go at it again some 4 or 5 hours later – while these guys spent sometimes 50-60% of their time leisurely surfing the internet. In some sense of the word, I consider this no less than stealing.

Misuse is defined as the improper or inappropriate use of the Internet and abuse is defined as using the Internet too often during company time. In the area of inappropriate surfing, a recent survey stated that one in three corporate workers said they spend 25 minutes or more each day using the Internet for personal reasons. Much of that time is spent shopping, with the most popular destination sites for vacations and vehicles. The study continued to say that employees report worse behavior among their colleagues. Nearly one in 10 respondents say they have seen co-workers accessing adult sites, while nearly one-third say they have seen co-workers job hunting on the Internet.

My company has policies in place along with login banners announcing that their equipment belongs to the US Government and that only work-related activities should be done – and that they should have no expectation of privacy. They are to agree to these terms before logging on. An example of a policy and perhaps a letter mailed to each employee's home could state: "With increased networking

capabilities, our desktop computers allow us to go almost anywhere in the world electronically. When used properly, these resources can provide significant benefits to The Company and to our customers. However, some individuals have ignored warnings and choose to use these resources improperly. Computing resources are for official business use in support of your assigned duties. You must not use computing resources in a manner which would constitute waste or fraud (such as playing games, viewing sexually explicit materials, or et cetera) toward the Department of Energy, the Company or any other government or commercial organization. Company computing resources must not be used to support any personal business or activities. If a computer is assigned to you, you are accountable for it and for how it is used. Anyone who uses computing resources for any purpose unrelated to his or her work should be prepared to accept the consequences, which range from a reprimand to dismissal, depending on the seriousness of the infraction. Anyone who has access to the Internet using Company' resources must be aware that transactions to and from the Internet are traceable and are routinely monitored. If you have access to the Internet, you should continue to take advantage of this extremely valuable tool for valid, appropriate, business-related activities. This resource is provided specifically so you can collaborate directly with your peers or obtain data from libraries and other resources. Inappropriate use of the Internet or other computing resources will not be tolerated. If you are uncertain whether your activities are work related, discuss the proposed activities with your supervisor. It is disappointing that the actions of a few may tarnish the reputation of the many who are working hard to produce quality products for our customers. When we use the Internet, let's do so as the professionals our co-workers and our customers expect us to be".

Last year (1999) 63 employees at my company lost their job for "misuse of government equipment", or in short, they were surfing the Internet; approximately 85% of these were downloading pornography. Having said all of that, when your employees abuse their Internet privileges, they put your company at risk for lawsuits (sexual harassment claims from pornography, and legal liabilities incurred from downloading objectionable or terroristic material). The worst cases I have been unlucky enough to be involved in have been

childporn cases. It's pretty scary to find that you are working side by side with a "Q-cleared" employee who has such a horrendous dark side. Fortunately, these employees are handed up to higher authorities and perhaps castigated from society altogether eventually.

Abuse of Internet privileges is potentially embarrassing to the entire organization. Sometimes companies with Web sites will publicize or make records available that show the addresses from which the majority of their users access their Web Page. An adult magazine recently published a list revealing that one of its major user groups accesses its Web site through a government agency's computer network.

In fact, the average cost of one potential legal liability case is $500,000! Some employees spend from 30 minutes to five hours a day surfing non-work related sites, and prime time surfing hours for the worst of the web is 9 to 5 - when most employees are hard at work!

According to various industry sources, one employee wasting an hour a day on the Internet can cost a company $6,000 a year. With 500 workers this is a $3 million a year problem. No wonder two-thirds of U.S. businesses block and monitor employee Internet usage.

Company integrity, productivity and monetary losses, and lawsuits are definitely areas of concern, but working in a Computer Security Organization, my main area of Internet heartburn is all the "scary" people lurking in the corners. I guess that through the years I have become more than a little paranoid about the nastiness that resides just a click away (and I "ain't" talking about porn).

If you are unfamiliar with a Web site or you notice any erratic behavior – go with your instincts – Get Out Now! Every day there are a ton of reports of new viruses, trojans, and scams. The Security Response Team (CSRT) has discovered a new strain of vandals (malicious auto-executable code) that attack computer systems through e-mail and web surfing. Aladdin reported the following on a new vandal: Far more advanced and dangerous than the notorious "BubbleBoy" vandal, the new threats come in many forms, including the "GodMessage"

vandal. The ability to embed any executable code into Visual Basic Scripts (VBS) sets the new strain of vandals apart from the BubbleBoy and other known threats to computer systems. New dangerous code engages in hostile activities ranging from installing a Trojan code that spy on user activities to completely destroying the hard drives and CMOS. These vandals have the potential to wreak havoc by changing system settings, emailing sensitive information, or destroying files before detection. The GodMessage vandal is unlike anything anti-virus vendors have previously faced because the hostile code is not embedded in an e-mail attachment. Traditional viruses residing in e-mail attachments must be opened to activate the virus. In contrast, vandals like GodMessage execute automatically the moment you view the email message. Users of Microsoft's Outlook® or Outlook Express® using the preview setting activate the vandal through the simple act of launching their e-mail application, thus enabling an embedded Visual Basic Script code to drop a malicious Trojan program in the Windows Startup folder. Auto-executable vandals can also attack systems while users are viewing an infected newsgroup message or an infected website. The hostile program, written in plaintext hexadecimal code, is embedded in the HTML source. A script converts the hexadecimal code into an executable file (EXE extension) and runs it. The script then erases all temporary files used, thereby removing any trace of its presence.

The vandal embedded in the GodMessage is only 8K in size, which is similar to a small GIF image. Upon execution it opens a custom FTP port to the victim PC, thus enabling a hacker to remotely download any file from users PC or upload and run malicious program at any time. Furthermore, the vandal notifies the hacker of the current victim's IP address each time the victim is online. This is done by sending an ICQ pager notification to a predefined ICQ number, allowing the hacker to install a more sophisticated Trojan like Back Orifice, Netbus or other malicious application at a later date. Other variants of the new vandal strain include:

- Trojanrunner98/NT, which downloads and runs a Trojan from an FTP site.
- Destroyer98/NT, which destroys the hard drive upon reboot.
- Experimental 98/NT, which starts deleting everything on drive C that is not running at the time.

- Annihilate 98/NT, which erases the hard drive and clears the BIOS.

Unfortunately, while cruising the highway, I landed on a well-known chat group which looked as if it dedicated most discussions to “how to” create trojans, etc.
(http://www.sotmesc.org/gcms/trojans/bbindex.html)

There are some serious software packages (thank goodness) that can be installed to detect and annihilate these types of vandals. In addition, firewalls can be installed to further thwart these activities

Although I may sound like an anti-Internet lunatic, I really don't regard the Internet as the malicious badguy on a rampage to eliminate our daily existence. Nor do I suggest interfering with Web development. I certainly applaud the great benefits we enjoy on a daily basis just in accessing needed information and keeping up with the latest and greatest in every imaginable field.

Electronic communication and information gathering is inevitably here for the everafter. However, we must remember that as we cruise the “highway”, we must adhere to all the road signs, pay attention to all posted cautions, and know when to slam on our brakes.

References:

Bacal, Robert " Q and A: Abuse Of Internet Access At Work - How To Address It” 22 Sept 2000
URL: http://www.themestream.com (01 Dec 2000)

National Consumers League/Dell “Consumer Guide to Internet Safety, Privacy and Security” 03 Oct 2000
URL:http://nclnet.org/essentials (01 Dec 2000)

PR CONNECTIONS [Johannesburg, 9 December 2000]
“Hitting the virus danger zone: New wave of auto-executables emerge”
URL: http://www.info-sec.com/virusses/99/viruses

Dennis, Sylvia “Nothing To Fear From Script Viruses, Says Sophos” 10 Oct 2000
URL: http://www.microtimes.com/newsfeeds/October2000/oct2000.html (12 Dec 2000)

Bator, Jane “National Steel Corporation Selects Telemate Net Software’s NetSpective™ to Monitor Compliance With Employee Internet Usage Policy” 06 Sep 2000

URL: http://www.telmate.net/pressroom/00-0009--06 12 Dec 2000)

Last Updated: July 23rd, 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 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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
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 Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
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
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 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