Securing Computers Connected to the Internet

CTAG Guide Document

For Public Distribution

Introduction

This paper has been produced to provide a high level guide to the implementation of secure unclassified Internet connections.

When planning and implementing an Internet connected network, it is often easy to leave out of miss something. Although most people know about Firewalls and Anti-Virus, they forget about maintenance contracts and the effect local laws might have on them.

In this paper we will attempt to highlight as many areas as possible and provide guidance to the issues raised.

Areas covered are as follows;

- Operating System
- Security updates
- Access Controls
- Anti-Virus
- Firewalls or ISP Routers
- General Risks

The information in this paper is applicable to either a single stand-alone PC connected to the Internet or a small network of Internet connected systems.

The Internet is not a safe place and this paper will attempt to enable the reader to make their system(s) more secure and protect their users.

An appendix at the end of this paper provides links to sites on the Internet with details of products covered.

Operating System

If a new system is being planned then the choice of Operating System, hardware and Internet Service Provider (ISP) are probably the main considerations, and so we will start there.

If the system or network is already in operation, then security and patching will be the top priority.

New Systems/Hardware

If new hardware is being purchased, in most cases it will come supplied with an operating system pre-loaded on it. The bulk of new systems have a version of the Microsoft Operating System, a few vendors will offer a Linux distribution and Apple computers come pre-installed with the Mac OS.

Linux is normally the cheaper option; it is a free operating system, but will require a level of skill to configure it that is often not available at small sites.

Apple Mac OS X is installed on all new Apple computers and is a stable Linux/Unix based Operating System (OS), which like Linux does require a level of administration skill not always available.

Microsoft's current Operating System (for desktop computers) is either Windows XP Home edition or XP Professional. It is recommended that the XP Professional version be purchased if possible, as it has better security options and offers greater flexibility.

It should be noted that the majority of attacks against computer systems are targeted against Microsoft Windows Operating Systems, Apple Mac and Linux (as desktop systems), are relatively secure and virus/spyware free. This should be factored in to the cost and administrative figures.

Existing Systems/Hardware

If existing computers are to be deployed, they will probably already have an Operating System installed on them.

It is good practice to format and re-install the Operating System to ensure that any sensitive data is not accessible on the computer.

Linux is a good option if old hardware is to be used. It often requires less memory and processor performance than the current Microsoft Operating systems and provides a very competent email and web-browsing Platform.

Security Patches

No software or Operating System is free from Bugs or vulnerabilities in the code. It is therefore of the utmost importance to ensure that the O.S. and Applications are patched when the vendor issues updates to the products.

Microsoft issue Service Packs for all their Operating systems, and the current one for the OS should be installed on all systems.

The Link below is to the Microsoft site and allows one to search for the current service pack for a product.
http://www.microsoft.com/technet/security/current.aspx

It is important to update the security packs for Internet Explorer (the Microsoft Web Browser) and Outlook (the email client). The site detailed above can provide information on the current patches for these applications.

Both Apple and Microsoft provide an automatic security update mechanism where Internet connected systems can download security patches on a scheduled basis.

To activate this on Microsoft products, select *Start - Programs – Control Panel – System – Automatic updates*.

On Apple Mac, from the Apple menu select *System Preferences – View – Software update*.

Linux systems will need to be updated manually, see the appropriate vendor web site (normally under a security sub menu) for details.

Access Controls

On a site where multiple users are permitted access to Internet connected system some form of access control must be implemented.

It is important that one can identify which user undertook what actions on a system, actions on the system must be accountable. If accounting is not undertaken, issues relating to offensive email, inappropriate material downloads or posting and issues of harassment can not be handled in a satisfactory manner.
This will then lead to problems if legal action is required.

User accounts should be set to logout after a certain period of inactivity to prevent accounts being misused.

Microsoft

With Microsoft systems, a nominated, trusted and authorised user only should use the administrative account. Users should not share accounts and if they do, separate (user-privileged) accounts should be configured for each individual.

Basic auditing should be enabled on each computer and logon/log off information, Management and Policy changes should be logged. This should be configured using the Windows NT Event log.
These logs must be checked on a regular basis for signs of misuse or attack.

Macintosh/Linux

As on a Microsoft system, only a nominated, trusted and authorised user should use the root account; all system users should have separate accounts configured for them. Users should not share accounts and if they do, separate (user-privileged) accounts should be configured for each individual.

The Syslog should be configured to capture login information, ensure that the *auth* line is set in the */etc/syslog.conf* file.

Anti-Virus

All system connected to the Internet should have an Anti-Virus (AV) package installed. The only case where this might not be applicable is on Read only (CD-ROM based Operating Systems or embedded devices with read only file systems. If files or email are going to be downloaded, then Anti-virus (AV) software should be installed. Although Virus and worms in the Mac/Linux world are less prolific, they still exist. It is also good practice to check incoming files and emails for viruses that effect other operating systems so that the user does not spread them to users on other systems.

AV should be configured to automatically update the virus definition files on a regular basis, (daily if possible).

Commercial Products

Most of the major Anti-Virus vendors provide packages for Microsoft, Macintosh and mainstream Linux/Unix systems. They average out at around fifty dollars for single system licences, this includes a years updates and maintenance patches. See the Mcafee website (www.mcafee.com), for details of one such product.

These applications will generally protect the user against Virus attacks, Internet Worms and some of the Trojan/software Key logger type attacks.

Free/Open Source Products

There are several companies offering 'free' Anti-virus for Windows users. The products are generally very good but the licensing agreements only allow the product to be used for personal use, not commercially.

Several Open Source AV offerings are also available, which might be suitable for small systems with budgetary constraints. The ClamAV product, (www.clamav.net) can run under all the main Operating Systems and the signature detection files are always very current.

Spyware

Spyware is another big issue on the Microsoft platform. There is a range of low cost products, which can detect and remove spyware from computers. If the systems are going to be predominantly used for web browsing it might be worth investing in one of these products, though Service Pack 2 for XP will help protect against this.

Firewalls/Intrusion Detection Systems

A Firewall is used to deny access to a computer system and protect it from out-side attack, (hackers).
Computers used to browse the Internet do not offer any Services (like a Web site from example) and so all in-bound connections can safely be dropped or blocked by a firewall.

ISP/Broadband

If the Internet connection is ADSL type broadband, then the easiest way to protect the computers is to install an ADSL router/firewall all-in-one unit.
These appliances can be purchased for about one hundred and fifty dollars and are simple to configure.
If an ISP has provided the connection, they will often supply a router or Firewall. Routers can be configured to block in-bound traffic in a similar manner to a Firewall. Many ISP's can or will configure the Router with Access Control Lists (ACL's) for you if asked.

Firewalls should also be configured on computers in-side the network, and defiantly on stand-alone dial-up systems.

Stand-alone Systems

Windows XP comes with its own Firewall called Internet Connection Firewall (ICF) which should be implemented.
For Microsoft Operating Systems prior to XP, (Windows 95 – Windows 2000) a Software firewall should be installed. These are available as commercial products or freeware. The freeware versions are normally licensed for personal use only.

Apple Mac OS X has a firewall that functions in a similar way to the Firewall on Windows XP.

Linux systems normally come with the Iptables filter as part of the distribution. Iptables is controlled via the command line but most versions of Linux provide a graphical tool that can be used to implement the Firewall rule-set with.

Risks

Surfing the Internet can become a very absorbing and time consuming operation. Does staff really require totally unrestricted access to the Internet. If they only need e-mail, remove the Web Browser or block Web access at the Firewall or Router.

Data from the Internet is often riddled with Trojans, spyware and viruses. Do not transfer this data to classified systems under any circumstances.

After using a computer to conduct Internet banking or any financial transaction, the user should clear the Web Browser cache. For users of Internet Explorer this can be accomplished by taking the following steps

1. Click on the **Tools** button on the Internet Explorer tool bar.
2. Highlight and click on **Internet Options** at the bottom of the Tools menu.
3. Under the **General** tab you will see "Temporary Internet Files" Click the **Delete Files** button.
4. Click **OK**

It is also good practice to delete the **Cookie** files and clear the **History** as well, also found under the **General** tab setting.

For users of the Firefox browser (which runs under Windows, Linux and Apple Mac – see ctag-0704.pdf), the settings are located under the **Tools Options Privacy** menu.

Appendix A

List of Internet base resources:

Microsoft

Service Pack locator
http://www.microsoft.com/technet/security/current.aspx

Security home page
http://www.microsoft.com/technet/security/current.aspx

Windows system admin security guidelines
http://csrc.nist.gov/itsec/

Apple Macintosh

Security home page
http://www.info.apple.com/usen/security/index.html

Linux

Redhat Security home page
http://www.redhat.com/security/

SuSe Security home page
http://www.suse.com/us/security/

Slackware Security advisories
http://www.slackware.org/security/

Anti-Virus

This site has details on all the major AV vendors
http://antivirus.about.com/od/antivirusvendors/

Firewalls/IDS

Good site with reviews and links to vendors products
http://www.firewallguide.com/software.htm

Policy Templates for IT Systems and Users

http://www.sans.org/resources/policies/