Global Information Assurance Certification Paper

Baseline Security for SMBs

By: David M. Cieslak, CPA, CITP

Assignment version # 1.3

Abstract

With the increasing availability and affordability of broadband access (DSL, cable modem, etc.) to the Internet, organizations of all sizes are now connected to the Internet 24x7. Accordingly, these organizations, along with their computing resources, are now exposed and at risk – especially if these organizations have not taken the necessary steps to protect themselves. Yet, due to limited technical and/or financial resources, many organizations, especially Small- to Medium-Sized Businesses (SMBs), don't undertake formal security assessments or even take the minimum essential steps to protect themselves from this growing risk. Whether it's avoidance, ignorance or simply a desire to focus on their core business, the net result is the same – they are left vulnerable to attack.

This paper proposes baseline security guidelines for SMBs based on industry "best practices." The items listed do not constitute a comprehensive list. And the recommendations listed are in no means meant to serve as a substitute for a formal security assessment. Instead, these recommendations are intended to provide minimum standards based upon the most common threats present on the Internet today and weaknesses noted in other typical SMBs. The information presented reflects information gathered from numerous resources as well as personal observation and experience consulting with hundreds of SMBs.

Background

Due to the affordability and availability of broadband access, more and more Small- to Medium-Sized Businesses (SMBs) are connecting their office networks to the Internet each day. This "always-on," high-speed access to the Web opens a whole new world of connectivity, information and opportunity for the SMB. Yet the Internet also presents a serious threat to the SMB's critical programs and data – and ultimately, their very business.

Interestingly enough, many SMB owners aren't even aware that their systems and data are vulnerable. They often pose questions such as "I have anti-virus software installed on my computer, aren't I safe?" or "Why would someone want to hack my system? Don't they only break into banks or big companies?" Unfortunately, the answer is a resounding "No!" The reality is all organizations, big and small, need to be concerned about information security.

The primary goals of information security are:

1. Confidentiality - information should only be available to authorized individuals.
2. Integrity - information should be modified only by those who are authorized to do so.
3. Availability - information should be accessible to those who need it when

they need it.

In order to address these goals, and begin to reduce the risks posed by the Internet, SMBs need to adopt multi-layered defense strategy. Specifically, SMBs should implement a number of fundamental practices and countermeasures in order to protect their information. It's important to note that no one action or product is wholly sufficient to protect an organization. Instead, by creating a multi-layered defense and using a variety of countermeasures, an organization can eliminate single points of failure and substantially strengthen their information security. SMBs should be able to implement the items presented at a reasonable cost.

What's an SMB?

While there is no standard definition for what constitutes a Small to Medium-Sized Business, government and market analysts generally classify SMBs as companies with fewer than 500 employees.

Given the size and number of employees, SMBs typically have workgroup-size networks comprised of either a Windows NT/2000 or Novell server, possibly a few specialty and/or support servers, along with Windows 9X/2000/XP workstations.

Baseline Security Recommendations:

While the following is hardly an exhaustive list, it does address several of the most common weaknesses facing SMBs, and therefore helps guard against some of the most prevalent threats facing these organizations.

- **Router and IP addressing**

  The first thing a SMB should have in place if they are accessing the Internet via a broadband connection is a router with NAT and DHCP capabilities. The router sits between the Internet broadband connection and the LAN. Fortunately, many SMBs already have a router in place because their broadband service provider or consultant installed one when the service was originally implemented. Surprisingly though, other SMBs do not have routers, often times because their broadband service providers discouraged their use – either because the service provider did not want to take responsibility for providing broadband connectivity to the entire LAN or because they wanted to sell multiple IP addresses to the customer – one for each end user.

  One of the benefits of using a broadband router is it allows multiple users to share a single public IP address, i.e. each user does not need to have their own public IP address in order to access the Internet. This is done by

assigning each user a unique internal IP addresses. Each of these internal IP addresses is then translated and forwarded by the router to a single shared external IP address when end users need to exchange information with the Web. This process of using one set of addresses for internal use and another address (or set of addresses) for external use and translating the information back and forth is known as Network Address Translation, or NAT. It's especially important to note that under most circumstances, internal users and devices should be given non-public, non-routable addresses. The Internet Assigned Numbers Authority (IANA) has pre-established several ranges of IP addresses as non-public and non-routable for this very purpose. They include:

- 10.0.0.0 – 10.255.255.255 (Class A)
- 172.16.0.0 – 172.31.255.255 (Class B)
- 192.168.0.0 – 192.168.255.255 (Class C)

By design, other routers on the Internet will drop traffic directed to these addresses since they are recognized as reserved for internal use. This ultimately prevents anyone on the Internet from directly accessing an end-user's machine that's using one of these special IP addresses.

A router can automatically assign an IP address to each internal user/device if it has DHCP capabilities. DHCP stands for Dynamic Host Configuration Protocol and can be used to automatically assign each device an IP address within a pre-designated range. The router then keeps track of which address is use by each device. When a device is turned off or disconnected, the IP address is returned to the pool and available for use by someone else.

Some of the more popular broadband router vendors include:

- Linksys – www.linksys.com
- Netgear – www.netgear.com
- DLink – www.dlink.com

Therefore, some of the benefits of using a broadband router with NAT and DHCP include:

- Reduced cost due to the ability to share a single public IP address between multiple internal users.
- Protection from direct outside access by others when using non-public, non-routable addresses on internal devices and using NAT to translate data back and forth to the shared external address.
- Reduced administration when using DHCP to assign IP address to each internal device.

- **Firewall**

Even though a broadband router with NAT capabilities provides basic protection by hiding internal IP addresses from the Internet, a dedicated

perimeter firewall provides additional functionality and security for a SMB. Specifically, a perimeter firewall sits between the Internet and end-users and allows only authorized data to move back and forth. Firewalls do this using one of several different methods:

- Packet filtering – Packet filtering firewalls are the most common. They review each data packet and accept or deny based on pre-established rule sets. When a packet is received, the address in the IP header is compared to an access control list to determine if it's permissible to accept the data.

  Although packet filtering firewalls are fast, they can be difficult to set up and maintain, and ultimately allow for a direct connection between source and destination computers potentially leaving them exposed.

- Stateful Inspection – Unlike packet filters that only examine the IP header of each packet, Stateful Inspection firewalls examine the contents as well, and only packets that belong to current connections, or sessions that have actually requested data, are allowed through. Stateful Inspection firewalls also provide added security by closing off all ports on the firewall until access is required. This minimizes exposure from port scanning. Stateful Inspection firewalls are quickly becoming the most popular.

- Application-level proxy – Application-level proxy firewalls determine if a connection to a given application or service is permitted, i.e. connectivity is controlled at the application level, such as Internet access, e-mail, ftp, etc. If communications are allowed, then the firewall further acts as a proxy on behalf of the requesting machine. In this environment, source and destination machines are never directly connected and all traffic flows through the proxy server. Proxy servers are the slowest and most difficult to set up.

In addition to the functionality outlined above, many of today's firewalls also include NAT and DHCP (similar to a broadband router) as well as logging, alerting, antivirus protection, content filtering, VPN, and DMZ support.

A list of ICSA Labs certified firewall products can be found at http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/index.shtml

- **Patches**

One key way that SMBs leave themselves vulnerable to attack is by failing to install the latest web browser, e-mail and operating system updates on all servers and workstations. In 2001 alone, 2,437[1] new vulnerabilities were

reported to CERT. Once discovered, software vendors work diligently to patch holes and usually make these fixes – sometimes also referred to as PTFs (Program Temporary Fixes), hot fixes or critical updates – freely available to end users over the Web. But many users do not apply these patches, and therefore unnecessarily leave themselves open to attack. In fact, SANS notes in their "Twenty Most Critical Internet Security Vulnerabilities" report, that "A few software vulnerabilities account for the majority of successful attacks" and that attackers "count on organizations not fixing the problems."[2]

Previously, many organizations took a "wait and see" approach to patches, i.e. wanted to see if a given patch made matters better or worse. Other organizations only installed patches after specifically encountering a given issue, or at the direction of a tech support representative. But given today's security climate, this is no longer a safe approach. Instead, patches should be installed as soon as they become available – especially those regarded as "critical" or that address security flaws in the operating system, e-mail client or web browser.

Users running Windows ME, Windows 98, Windows 2000 or Windows XP can visit http://windowsupdate.microsoft.com or simply run the built-in *Windows Update* function by clicking "Start" then selecting "Windows Update" to determine which critical updates are missing and should be applied.

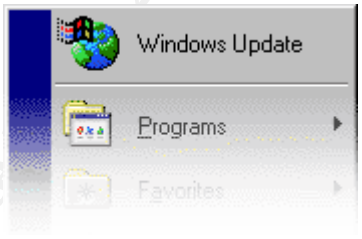

Figure 1[3]

Another useful tool for determining if all critical patches have been applied to Windows NT, 2000 and XP workstations is the Microsoft Personal Security Advisor (http://www.microsoft.com/technet/mpsa/start.asp).

Machines running different versions of Windows or other operating systems can use a variety of commercial and/or free tools to help determine which of the latest critical updates are necessary. A partial list of these tools includes:

Windows-only:

- HFNetChk – http://www.microsoft.com (NT 4.0/2000/XP)
- BigFix – http://www.bigfix.com (95/98/ME/2000/XP)
- Hercules – http://www.citadel.com (NT/2000/XP)
- Update Expert – http://www.stbernard.com (NT/2000/XP)
- Service Pack Manager – http://www.securitybastion.com (NT/2000/XP)

Hotfix Control – http://www.nttoolbox.com (NT 4.0)

Windows + other platforms/services:
Retina – http://www.eeye.com/html/Products/Retina/index.html
CyperCop – http://www.pgp.com/products/cybercop-scanner/default.asp

Note: Several of the tools listed above are capable of performing much more comprehensive vulnerability scanning of various systems and services, but at the very least, could and should be used to determine which critical updates need to be applied. If users have questions about specific products or vendors, they should directly visit the vendor's web site to check for any relevant security patches.

- **Anti-virus**

Viruses are probably one of the most well-known and prolific threats to information security. Symptoms of infection can range from mildly annoying (such as displaying a message every time a key is pressed) to highly damaging (destroying the operating system or wiping out an entire disk volume). And while some viruses are more destructive than others, there is no such a thing as a "good virus" as they all constitute the unauthorized or unintended use of a user's machine.[4]

How extensive are viruses? Well, there are over 60,000[5] known viruses in existence today with hundreds more being added each month.

How are systems infected? Viruses can be introduced from virtually any outside source, but the highest threat vectors presently are e-mail, Internet downloads and web browsing.[6] Once infected, the compromised machine then places other computers on the same network at greater risk.

The word "virus" is often used globally to refer to any type of malware (malicious software) that threatens a user's machine. But it's important to note that viruses are actually just one type of malware. Worms, Trojans and other malicious applets are increasing in popularity and frequency and also putting systems at risk. Basic definitions for the various types of malware are as follows:

- Virus - A computer program file capable of attaching to disks or other files and replicating itself repeatedly, without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies or creates the files.[7] Viruses can be further classified as:
  - Boot Sector – virus is located in the hard drive boot sector and

loaded into memory when the computer boots. [7]
    - File - Usually replace or attach themselves to COM and EXE files. They can also infect files with the extensions SYS, DRV, BIN, OVL and OVY. Many non-resident viruses simply infect one or more files whenever an infected file runs. [7]
    - Macro - A malicious macro written using a macro programming language and attached to a document file (such as Word or Excel). When a document or template containing the macro virus is opened in the target application, the virus runs, does its damage and copies itself into other documents. Continual use of the program results in the spread of the virus. [7]
    - Companion - Companion viruses use a feature of DOS that allows software programs with the same name, but with different extensions, to operate with different priorities. Most companion viruses create a COM file which has a higher priority than an EXE file with the same name. [7]
    - Script – targeted at machines running Windows Scripting Host, use standalone Visual Basic Script (VBS) and JavaScript (JS) programs to execute malicious commands. [4]
- Worm – a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems without user action or intervention. The propagation usually takes place via network connections or e-mail attachments. [8]
- Trojan – also known as a Trojan horse, appears as a seemingly harmless program or data file, but contains malicious code. Trojans are becoming increasingly more sophisticated and potent and many now look to hijack target machines. A few notable Trojans are Back Orifice, NetBus and Sub Seven.

In order to best protect themselves from viruses, worms and Trojans, SMBs should take the following steps:

- Install anti-virus software on all client workstations, network servers and any e-mail server(s) with real-time scanning turned on.
- Perform complete system scans on a regular, scheduled basis with results written to a log file.
- Update virus signatures weekly. Push updates to client machines whenever possible to manage the process and ensure that virus signature files are up to date.
- If using Microsoft Office products, verify that macro security is set to the medium or high level in order to warn user when opening files with macros.
- Scan all e-mail / attachments prior to opening
- Instruct users to not open e-mail / attachments from unknown senders
- Turn off the Windows Scripting Host functionality to prevent script viruses from running. [9]

Some of the more popular anti-virus vendors and products include:

- Symantec – http://www.symantec.com
- McAfee – http://www.mcafee.com
- Computer Associates – http://www.cai.com
- Trend Micro – http://www.antivirus.com

More complete listings of anti-virus vendors and products may be found at:

- http://www.icsalabs.com/html/communities/antivirus/certifiedproducts.shtml
- http://csrc.nist.gov/virus/
- http://www.cert.org/other_sources/viruses.html#I

- **Passwords**

Passwords are an essential aspect of information security, whether connecting to an internal network or resources on the Internet. Yet for many SMBs, missing or weak passwords can place critical systems at risk and unnecessarily jeopardize confidential information. Therefore, it's essential that SMBs implement strong passwords to protect themselves and their data.

While there is no authoritative list, security professionals generally agree on the following guidelines and criteria regarding passwords:

- Passwords are required for all accounts, sites and services
- Null (blank) passwords are not allowed
- Use different passwords for each account, site and service
- Don't use passwords that are easy to guess, i.e. names, birthdays, anniversaries, pets, hobbies, office objects, etc.
- Don't use words found in the dictionary – any dictionary, domestic or foreign
- Don't use vendor-supplied default passwords
- Change passwords at least every 90 days
- Passwords should be at least 7 characters long
- Password should include a mixture of upper and lower case letters if supported
- Passwords should include at least one number and one symbol/extended character when possible
- Don't write passwords down – especially on a sticky note near the machine.
- Don't share passwords
- Maintain password history to prevent users from re-using their last 10 passwords
- Change a user's password or remove their account entirely when they

leave the company

It's important to note that any password – even the most complex ones -- can be cracked given enough time and computing resources. But by following the criteria outlined above, users can create sufficiently strong passwords that then play an important role in helping protect sensitive information.

- **Limit services**

By default, operating systems install a variety of applications and services during the initial installation process. While some of these applications and services are essential in order for the operating system to function properly, others, such as web services, ftp, remote access, etc., are optional and often not required by many end users. Unfortunately, end users are often unaware these services have been installed, and are now presently active on their machines. Accordingly, attackers scan for these services and the open ports they run on. They prey on the fact that end users have performed "generic" operating system installations and aren't patching vulnerabilities presented by these unused services or monitoring the activity on related ports.

How can users protect themselves? By reviewing applications and services running on their machines, turning off all non-essential services and closing extraneous ports. There are a number of free and commercially available tools that enable users to scan machines and list services running and the corresponding open port(s). Some of the more common tools include:

- Active Ports (http://www.ntutility.com/freeware.html)
- NMapNT (http://www.eeye.com/html/Research/Tools/nmapNT.html)
- FPort (http://www.foundstone.com/knowledge/free_tools.html)

Using the output provided, users can then turn off services and close ports they don't require.

- **Unprotected Shares**

Occasionally, users in workgroup environments need to share local resources (files and printers) with other users. And Microsoft Windows makes the sharing of resources simple to do. But unfortunately, rather than sharing specific limited resources, i.e. a given file or folder, end users instead often share entire disk volumes. Compounding matters, they don't require guests to authenticate themselves in order to access these shared resources. Finally, users often use the NetBIOS protocol to share these resources. The net result is they unnecessarily make their systems vulnerable to attack, especially when the local area network is connected to the Internet. Therefore, users should consider the following to secure against possible unprotected shares:

If file sharing IS required:

- Require passwords to connect
- Ensure only required directories are shared
- Use file system permissions to ensure that proper access is provided to authorized users
- Use NetBIOS only if necessary
- Block inbound and outbound NetBIOS traffic (TCP and UDP ports 137 through 139 and 445) on the perimeter firewall if NetBIOS is used.
- For workstations running Windows NT, 2000 and XP, modify the registry to restrict anonymous logons. This will prevent null session connections to these machines and the ability for attackers to enumerate users, groups, system configuration information and certain registry keys.

If file sharing is NOT required:

- Disable Windows networking shares or consider disabling NetBIOS over TCP/IP altogether in the Windows network control panel.

Users can run the Microsoft Personal Security Advisor (if using Windows NT, 2000 or XP) located at http://www.microsoft.com/technet/mpsa/start.asp to determine if a machine is vulnerable. Note: this is also an excellent tool for determining various overall machine vulnerabilities.

- **Personal firewalls**

In addition to a perimeter firewall, SMBs should consider installing personal firewall software on each end-user workstation. Personal firewalls provide an extra layer of protection and keep unauthorized data from entering or exiting end user's machines.

Some of the benefits provided by personal firewalls include:

- Guarding users from LAN-based attacks, i.e. originating inside the perimeter firewall
- Protection from accidentally downloaded Trojan horse programs (via e-mail, chat, etc.)
- Protection from hostile cookies and browser code
- End-user confirmation for applications attempting to access the Internet
- Alerting user to port scanning activity

Additionally, personal firewall products may also provide:

- Virus protection

- Malicious script filtering
- E-mail attachment filtering
- Ad filtering
- Cookie control

As of March 2002, ICSA Labs certified the following personal firewall products (http://www.icsalabs.com/html/communities/pcfirewalls/cert_prods.shtml):

- Sygate Personal Firewall Pro by Sygate Technologies, Inc.
- Norton Personal Firewall 2002 by Symantec Corporation
- Tiny Personal Firewall by Tiny Software
- Zone Alarm Pro by Zone Labs

Additional information on personal firewalls and other products can be found at http://www.firewallguide.com/software.htm.

- **Web-based e-mail**

End-user use of web-based e-mail products, such as Yahoo, Hotmail and Excite, presents a potentially significant security threat to SMBs since these programs operate almost entirely outside the security infrastructure of an organization. Inbound web-based e-mail may contain viruses, worms or Trojans that could go undetected and ultimately infect end-user machines and potentially an entire LAN. Outbound web-based e-mail allows for the possibility of inappropriate communications, i.e. confidential information is shared with outside parties.

Ideally, SMBs would check all inbound e-mail for possible viruses, worms, Trojans and other malware as well as filter out spam, junk mail and other inappropriate content by employing the following strategy:

- E-mail is scanned for both viruses and spam when downloaded to the corporate e-mail server using server-based software.
- E-mail is scanned again by anti-virus software located on each workstation when end-users open individual messages.

Since web-based e-mail programs do not send messages through corporate e-mail servers, but instead send and receive messages via port 80 (HTTP), content and attachments are able to freely move between the Internet and end-user machines without being scanned for viruses by the corporate mail server. As a result, spam, junk mail and malware can be delivered directly to the end user's desktop.

In order to minimize the threat, SMBs should consider adopting the following policies:

- Unless absolutely required, end users should be prohibited from using web-based e-mail programs.

- If web-based e-mail is permitted, attachments should not be opened or executed without being saved and scanned for viruses first. Note: it's crucial to keep workstation anti-virus signatures up to date since this may represent the only line of defense against malware.
- Real-time antivirus scanning should be active at all times on end-user workstations.
- Users should be educated on the possible dangers presented by web-based e-mail solutions.

Note: In order to actively prohibit the use of web-based e-mail, organizations can do the following:

- Workstation browser software can be configured to restrict access to web-based e-mail sites.
- Perimeter firewalls or filtering routers can be configured to block access to web-based e-mail servers. Note: if IP address information is entered incorrectly or too broad in scope, other legitimate web access may also be blocked.
- Internet filtering/monitoring software, such as SuperScout Web Filter (http://www.surfcontrol.com), WebSense (http://www.websense.com) or Elron Internet Manager (http://www.elronsw.com) can be used to restrict access.

Note: Instant messaging (IM) programs such as Yahoo, AOL, ICQ and Microsoft Messenger as well as peer-to-peer file sharing programs such as Morpheus, Gnutella, Bear Share and KaZaA present similar possible security threats and their use should also be evaluated by SMBs in a similar way.

- **Backups**

Creating a layered defense to guard against attacks is important, but the ability to recover if and when systems are compromised is no less essential. In fact, sound backup and restore procedures are crucial to ensure the continued availability and integrity of critical programs and data in the event of breach. Without adequate backup and restore procedures, small problems can snowball into major ones!

There are several basic types of backup:

1. Full – All information is backed up, regardless of whether it was changed. Note: this is the most time-consuming type of backup, but the simplest from which to restore.
2. Differential – All data that has changed since the last full backup is saved.
3. Incremental – All data that has changed since the last full or differential backup is saved. Note: this is the quickest to perform, but most difficult to restore from since the last full backup must be

restored first, then each incremental backup must be restored.

4. Image – an entire image of a disk volume is stored.

It's also important to note that various media can be used for data backups, such as tape, zip disks, CD-RW and other hard drives. The media used should compliment the amount of data that needs to be backed up, i.e. small, slow media should not be used to back up large amounts of information.

In order to provide sufficient protection, SMBs should have a comprehensive backup policy that includes the following:

- Key Data – key data needs to be identified, i.e. which server and/or workstations does key information reside on?
- Automatic – backup software with automatic scheduling capabilities should be used to create and run backup jobs.
- Regular – key data should be backed up daily.
- Full – full server backups should be done at least once a week
- Rotation – multiple media sets should be used and rotated, i.e. today's backup should not be overwritten on yesterday's media. A minimum two week media rotation, with a separate month-end set is recommended.
- Secure – media should be stored in a secure location once backups are completed and verified.
- Off-site – a full backup should be regularly rotated to an off-site storage location for use in case of catastrophic disaster.
- Tested – test restores should be done at least monthly to ensure backups are valid and useable.
- Logs – backup logs should be used to track date, media, method (full, differential or incremental) and status (successful or failed).
- Images – disk images should made after new machines are configured and ready to place in service. This allows users to quickly restore machines back to their original state.

References:

General

The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated). The Experts Consensus." Version 2.502. January 30, 2002. http://www.sans.org/top20.htm

Carnegie Mellon University. "Home Network Security." December 5, 2001. http://www.cert.org/tech_tips/home_networks.html

Microsoft, Inc. "Safe Internet: Microsoft Privacy & Security Fundamentals – Security Best Practices Checklist." April 2, 2002. http://www.microsoft.com/privacy/safeinternet/security/best_practices

Router and IP addressing

Crider, Daniel. "A 6-Layer Defense for an I.T. Professional's Home Network." November 22, 2001. http://rr.sans.org/homeoffice/6layer.php

Brown, Bruce and Brown, Marge. "SOHO Security." Extreme Tech. February 27, 2002. http://www.extremetech.com/print_article/0,3428,a=23325,00.asp

Firewall

Hazari, Sunil. "Firewalls for Beginners." November 6, 2000. http://online.securityfocus.com/infocus/1182

Sonic Wall, Inc. "Internet Security Issues and Solutions for Small and Medium Business." April 1, 2002. ftp://ftp.sonicwall.com/pub/info/SME_WP.pdf

Digiterra Broadband. "Broadband Internet Security Basics." April 1, 2002. http://www.cable-modem.net/features/mar00/story1.html

Patches

[1] http://www.cert.org/stats/cert_stats.html#vulnerabilities

[2] The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated). The Experts Consensus." Version 2.502. January 30, 2002. http://www.sans.org/top20.htm

[3] Trend Microsystems. "Safe Computing Guide." http://www.antivirus.com/vinfo/safe_computing/#7

Carnegie Mellon University. "Home Network Security." December 5, 2001. http://www.cert.org/tech_tips/home_networks.html

Zocco, Paul A. "Ten Days to Network Security." August 6, 2001. http://rr.sans.org/securitybasics/10days.php

Viruses

[4] Computer Associates International, Inc. "Computer Viruses – An Introduction." October 18, 2001. http://www3.ca.com/Solutions/Collateral.asp?ID=897&PID

[5] http://vil.nai.com/vil.default.asp

[6] Bridwell, Lawrence M. and Tippett, Peter MD, Phd. "ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001."

[7] McAfee. "Virus Glossary of Terms." http://www.mcafee.com/anti-virus/virus_glossary.asp?

[8] http://www.antivirus.com/vinfo/virusencyclo/glossary.asp#virus_types

[9] Trend Microsystems. "Safe Computing Guide." http://www.antivirus.com/vinfo/safe_computing/#1

Zocco, Paul A. "Ten Days to Network Security." August 6, 2001. http://rr.sans.org/securitybasics/10days.php

Passwords

Microsoft, Inc. "Safe Internet: Microsoft Privacy & Security Fundamentals – Security Practices Checklist - Use Strong Passwords." http://www.microsoft.com/privacy/safeinternet/security/best_practices/passwords.htm

Donovan, Craig. "Strong Passwords." June 2, 2001. http://rr.sans.org/policy/password.php

M-Tech, Mercury Information Technology, Inc. "Password Management Best Practices." February 5, 2000. http://www.psynch.com/docs/best_practices.pdf

Limit services

The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated). The Experts Consensus." Version 2.502. January 20, 2001. http://www.sans.org/top20.htm

Rolling, Greg. "Security for Small and New IT Departments: Get Your Big Rocks in First." July 13, 2001. http://rr.sans.org/securitybasics/IT_dept.php

Unprotected Shares

The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated). The Experts Consensus." Version 2.502. January 20, 2001. http://www.sans.org/top20.htm

Carnegie Mellon University. "CERT Incident Note IN-2000-02." April 7, 2000. http://www.cert.org/incident_notes/IN-2000-02.html

Personal firewalls

Crider, Daniel. "A 6-Layer Defense for an I.T. Professional's Home Network." November 22, 2001. http://rr.sans.org/homeoffice/6layer.php

McDougall, Bonnie. "Personal Firewalls – Protecting the Home Internet User." August 17, 2001. http://rr.sans.org/firewall/home_user.php

Web-based e-mail

Trombold, Eric. "The Security Implications of Web Based Email." July 22, 2001. http://rr.sans.org/email/web_email.php

Backups

Rolling, Greg. "Security for Small and New IT Departments: Get Your Big Rocks in First." July 13, 2001. http://rr.sans.org/securitybasics/IT_dept.php

The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated). The Experts Consensus." Version 2.502. January 20, 2001. http://www.sans.org/top20.htm

Carnegie Mellon University. "Configure computers for file backup." June 12, 2000. http://www.cert.org/security-improvement/practices/p071.html

Last Updated: July 27th, 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
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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 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
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
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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS