Global Information Assurance Certification Paper

How to Create and Deploy a Successful Patch Management Policy and Program

Written By:
Felix Foret

Patch management can be the difference between a company running a successful IT department or a failing IT department. It is only a matter of time before a virus or hacker exploits security vulnerability at your company. Small companies working out of a single building to large companies working in multiple countries can benefit from having a patch management process in place. A viruses or security vulnerability has the ability to infect a company within minutes and cost the company millions of dollars. For this reason alone patch management has become even more valuable. First, I will discuss viruses and security vulnerability that can affect computers. Second, I will look at how patch management can affect your company. Third, I will discuss important parts of policies and procedures for setting up a successful patch management system. Finally, I will cover the different types of patch management software endorsed by Microsoft's.

Some people think we are on the verge of a horrific cyber disaster. I feel the disaster will come in the form of a super worm or computer virus. In the very near future super worms or computer viruses will be faster and more destructive then any previous virus seen before. The super worm or computer virus will be more intelligent and be able to change its structure in order to avoid detection. What is a virus? According to Trend Micro, "A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual." [1]

Most people think viruses have not been around very long, but that is not the case. Computer viruses have been around as long as computers have been in use. One of the first virus attacks recorded was in the early 1980's on an IBM computer. This virus did not have a big impact since the internet was sill in it infancy. Each year the total number of virus and security vulnerabilities grows even larger than the year before. According to CERT/CC statistics from 1988-2003 the total number of incidents recorded grew every year since they started keeping records in 1988.

[1] Virus Primer http://www.trendmicro.com/en/security/general/virus/overview.htm)

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	1Q-3Q 2003
Incidents	21,756	52,658	82,094	114,855

Total incidents reported (1988-3Q 2003): 297,318[2]

The Computer Security Institute teamed up with the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 12 March 2001, to investigate virus attacks and security breaches listed below are the results of their findings.

- 85% (primarily large corporations and government agencies) detected computer security breaches within the last twelve months
- 64% acknowledged financial losses due to computer breaches
- 35% (186 respondents) were willing and/or able to quantify their financial losses. These 186 respondents reported $377,828,700 in financial losses. (In contrast, the losses from 249 respondents in 2000 totaled only $265,589,940. The average annual total over the three years prior to 2000 was $120,240,180.)
- The most serious financial losses occurred through theft of proprietary information (34 respondents reported $151,230,100) and financial fraud (21 respondents reported $92,935,500).
- More respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%).

[2] **Cert/CC Statistics 1988-2003**
http://www.cert.org/stats/cert_stats.html

- The rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001.
- 36% reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)
- 40% detected system penetration from the outside (only 25% reported system penetration in 2000).
- 38% detected denial of service attacks (only 27% reported denial of service in 2000).
- 91% detected employee abuse of Internet access privileges (79% detected net abuse in 2000)
- 95% detected computer viruses (only 85% detected them in 2000).

Related to e-Commerce:

- 97% have WWW sites.
- 47% conduct electronic commerce on their sites.
- 23% suffered unauthorized access or misuse within the last twelve months.
- 27% said that they didn't know if there had been unauthorized access or misuse.
- 21% of those acknowledging attacks reported from two to five incidents.
- 58% reported ten or more incidents.
- 90% of those attacked reported [web site] vandalism (only 64% in 2000).
- 78% reported denial of service (only 60% in 2000).
- 13% reported theft of transaction information (only 8% in 2000).
- 8% reported financial fraud (only 3% in 2000).[3]

As you see from the chart virus incidents have more than doubled every year since 1999. Today, it is a rare occasion when a new critical virus or security vulnerability is not brought to everyone's attention either by the media, software vendor, email, or word of mouth. Viruses and security holes are costing companies billions of dollars world wide. SANS and the FBI have teamed up to produced a list of the top ten vulnerabilities that plague users today. This list shows vulnerabilities that would allow a hacker or a virus to compromise a home user or a large company network. Listed below are the top ten vulnerabilities that are considered to be used the most by viruses and hackers.

[3] General Information Security Statistics:
http://www.securitystats.com/infosec.html

SANS/FBI list the top 10 actively exploited Windows Threats.

1. Internet Information Services (IIS)
2. Microsoft SQL Server (MSSQL)
3. Windows authentication
4. Internet Explorer (IE)
5. Windows remote access services
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook and Outlook Express
9. Windows peer-to-peer file sharing (P2P)
10. Simple Network Management Protocol (SNMP)[4]

A virus or security vulnerability can infect your company in many different ways. They can come into your network via floppy disk, email, or by P2P (peer-to-peer) networking. Computer viruses are mainly transferred through email and P2P networks. When viruses spread by using email or P2P networking the rate of infection rises exponentially. This is evident from the virus *SoBIG* and *SQL Slammer Worm* which spread throughout the internet at speeds never seen before. As of today *SoBig* and *SQL Slammer Worm* have been the fastest spreading email virus and virus worm to date. It took the SQL Slammer worm ten minutes to spread worldwide. The worm doubled the number of computers infected every 8.5 seconds and by the time the worm reached it peak it was scanning 55 million IP addresses every second. Viruses can have a major impact to your company in many different aspects. They impact users, the IT department, and the company's bottom line. Users are impacted because they run the risk of losing all of their data. This can be very disruptive to someone who has extremely important data. Viruses can have a big impact on the IT department. Once a virus infects a company network the IT department must do everything possible to either control or eradicate the virus from the company network. I have seen some IT departments work 48 hours straight to control a virus that has the ability to spread fast and potentially be damaging to users files. A virus can have an enormous impact on a company's bottom line. In the past there have been many computer viruses that have spread throughout the world and do nothing more than slow down your company network connection or your internet connection. These viruses are usually more annoying than destructive but can still hit a company's bottom line pretty hard. They have the ability to produce enough network traffic to the point where servers have to be completely removed from the network. There have been

[4] **Top Vulnerabilities to Windows Systems**
http://www.sans.org/top20/

situations where a company was attacked using a large number of computers to produce a denial-of service attack. A denial-of service attack is designed to flood a server so that it cannot perform any other function then to process what you are flooding it with. This in effect denies service to those who would normally be using the server. DOS, denial-of-service attacks can be extremely costly especially if you rely heavily on your servers to produce income. Attacks can be costly but there is an even more destructive side to some viruses. Some viruses have the ability to infect system files and take down a computer or server. As of today there has never been a complete eradication of any virus. Most of the older viruses just fade away. This is one of the main reasons your company should implement a patch management program.

Patch management is the process of applying security fixes also known as hot fixes to a computer or a company network computer by using a detailed process and specific patch management software. It is no hidden secret that the majority of software written today has some type of vulnerability. Software vulnerabilities have doubled every year since 1999 and at today's current rate 2003 will be no different. It is estimated that five to 20 bugs are in every 1,000 lines of code in published software. Knowing this information viruses are not going away anytime soon. "There have been more than 60,000 viruses identified and 400 new viruses are created each month."[5] Companies are trying to stay ahead and keep their vulnerability to a minimum. Patches are created to fix holes in software that would allow someone to gain access to your computer. These holes can be used by hackers to either execute code or obtain information. Due to the recent virus outbreaks, patch management has become even more important and challenging. Recent viruses like SQL Slammer and MS Blaster have demonstrated to companies that their networks can be crippled or even taken down by a computer virus.

The benefits of a patch management program can be seen in lower operating cost of your IT department, an increase in the IT staff's productivity, and the increase in the moral of your IT department. A quality patch management program can lower your IT departments operating cost due the number of techs required to deploy a patch. It is no secret that most companies are down sizing and the IT departments are taking their fair share of employee cut backs. These layoffs have placed even more demand on individuals to handle more computer issues in this fast pace, I need it fix right now, business world. By implementing a patch management process you can reduce the amount of time patching places on your

[5] Virus Primer
http://www.trendmicro.com/en/security/general/virus/overview.htm

local IT tech. If you are manually installing patches, deployment cost can skyrocket when you take into consideration it takes on average three to five minutes to download the security patch, install the security patch, and reboot the computer after the installation. A properly executed patch management program allows you to scan every computer on the network, install multiple patches without rebooting after each patch installation, and schedule reboots after hours. The patch management deployment process can be done silently in the background without anyone knowing. Another benefit of a patch management program is the ability to schedule reboots after hours. When your patch management program is working properly the amount of hours the local tech spends deploying patches will decline as well. This will allow the local tech to concentrate on daily trouble tickets submitted by end users. Allowing techs to concentrate on daily trouble tickets will also improve SLAs (Service Level Agreements). Since there are viruses and security updates released weekly using a manual approach to patch management may have a damaging affect on your IT staff's morale. The manual deployment strategy requires a lot of man hours and the work is tedious to most IT tech.

In my opinion, viruses and security vulnerabilities would not be as big of an issue if everyone was forced to use an anti-virus software program and have all critical patches installed before they could connect to the internet. In the past, Microsoft has released as many as five patches or alerts in one week. If you do not have a patch management policy in place you could be facing immediate danger from every email an employee opens and every download they launch. Knowing your company is doing everything to protect itself from viruses and security vulnerabilities is one of the main reasons you should implement a patch management policy. Patch management has become increasingly popular since some companies have lost millions of dollars in lost productivity. Historically most companies did not have a patch management program or it was left up to the local IT tech. Some companies continue to allow this function to be carried out by the end user. This is not a good idea even if you configure windows to automatically download the patch installation. Once the patch is downloaded the user receives a pop up window which most users immediately dismiss leaving the patch uninstalled. Allowing the user to execute this function really places a company in a vulnerable position. Giving end user the right to decide if your network will be protected by installing a security patch is like playing Russian roulette. The old sneaker net install approach (a tech touching every computer) is still being used by some companies today. While this is very time consuming it is still better than nothing.

Patch management policy will give your company a structured program to be able to protect itself from viruses and security vulnerabilities. Also, a patch management policy will enable you to use your time wisely and become more cost effective. Since there is no policy that will fit every company we will cover some of the major points that need to be in your patch management policy. Your patch management policy should cover in detail the steps to be used to implement and execute a successful patch management program. It is important to note that this policy must be approved by all management personnel including the CEO or Owner of the company. If you do not have the backing of the CEO or owner of the company no one will feel like they have to follow the policy. Patch management policy can only be effective if it is strictly enforced.

While it is hard to find information on patch management or patch management policy, ISO 17799, *Code of Practice for Information Security Management*, can assist your company in developing a successful patch management program. (ieee3-13) Patch management policy will differ from company to company based on size, geography, personnel and so forth. Almost every key point of your policy will rely on other key points to ensure you are successful at deploying a patch. Some of your company's patch management policy guidelines might include guidelines for the responsibilities, testing, and deployment procedures for your patch management program. A good practice is to be able to use time lines in order to improve your company's ability to apply a viruses or security patch. Where practical there should be more than one person responsible for any of these guidelines. A good plan of action is to have multiple people on each team and each team has backup for each role on the team.

Responsibilities will need to be assigned to an individual or to members of your IT department explaining their roles from the beginning to the end of a patch deployment. Your policy should address who will be responsible for monitoring, testing, patch deployment and deployment alternatives when new viruses or security vulnerabilities are released. The creation of a monitoring team can mean the difference between success and failure. By monitoring viruses or security vulnerabilities you will be ready to start testing patches as soon as a patch is available to the public. Using a reactive approach will place strain on other parts of your program. Sometimes you have only hours before a virus is discovered but there are times when you have days even months before a known viruses or security vulnerabilities becomes a threat. For example, patches for Code Red had been out for months before the attacked was launched. The amount of time an IT administrator has to test the patch was considerably longer than normal. Even though a patch was available for months there were still over 115,000 websites attacked by Code Red. (1-1a) There should never be only one person responsible

for monitoring new viruses and security vulnerabilities. You should always have a backup person should be designed in case of a vacancy in that role.

Testing each and every patch can be one of the most important parts of your patch management policy. Testing can be a long and stressful part of your patch management policy but can prove to be the most cost effective. In the past Microsoft has been known to release patches that have created other issues in the windows operating system platform. Some of these issues have resulted in the dreaded Blue Screen of Death. Since time is usually critical when a patch is released, developing a top notch testing lab will make your program even more successful. You should test every patch before deployment. Testing can mean the difference between successful patch deployments or a company loosing millions due to down time. A lot of companies use proprietary software that is created by their programming department. Since some patches can have a damaging affect on computers it is extremely wise to install patches in a test environment. The test lab should exactly simulate your company's computers and network structure. There have been many situations where a non-production test passes but the live test fails. For this reason, it is wise to perform a small sample test on your live production network. The objective is to take a small sample of computers that are used on a daily bases and install the patch. This will give you a real world testing environment on a live production network and give you confidence that deployment will be successful. Of course you will only be able to perform this test if time allows and it is always smart to have a back out plan should your live test fail.

Deployment procedures will rely heavily on monitoring and test guidelines established by your patch management policy. Deployment procedure guidelines define how every patch will be deployed. There are many different ways to deploy the latest virus or security patch. A patch can be applied manually or software can be used to automate the install process. As mentioned earlier, some companies still use the manual approach. There are some benefits to this approach but at some point the cost will out way the benefits. With the number of viruses and security vulnerabilities being discovered today the automated approach has become a major part of the typical IT department. Another guideline that falls under the deployment procedure that needs to be addressed is centralization or decentralization. Your company needs to decide if you are going to run your patch management program from a main location or multiple locations. There are pros and cons to both sides. Many companies have gone to a centralized decentralized process. For example, servers are patched from a central location and desktops are patched by the local desk top tech. This practice seems to be more efficient when a virus or security vulnerability is at the mission critical level.

There are many other guidelines that should be addressed in your patch management policy. Here are some examples of guidelines that you might want to include in your company's patch management policy, VPN guidelines; firewall setup and management, patch deployment schedules, email attachments, and auditing guidelines just to name a few. Most companies with large networks give their employees the ability to access the company's network through a virtual private network connection or VPN. Since these users usually work at home having the ability to install a virus or security patch can be critical. Working closely with the team that maintains the company firewall can reduce your company's exposure to known viruses or security vulnerabilities. Insuring your company's firewall is setup correctly and maintained on a timely bases can mean the difference between applying the latest virus or security patch without the fear of exposure. Designing a patch deployment schedule will depend on how mission critical a patch deployment is to your company network. It is important to take into account bandwidth usage, risk of data lost, and loss productivity. Scheduling patch deployment after hours can go along way to improving bandwidth usage, data loss, and loss productivity not to mention user's (what they think) about the IT department. Email attachments should be monitored closely. Today, most company email servers block certain types of attachments. These attachments are blocked because they have file extension that are associated with viruses and security vulnerabilities. Some of these attachments sent through email might be valid but it is believed better safe than sorry. During a patch deployment the auditing process should be performed at least once a day. Extremely critical situations will require more frequent audits. The audits should be designed to monitor the patch deployment process and give you certain information about the computers on your network by name. Using an automated process to display the total number computers scanned on your network, display computers scanned for applied patches, total number of computers the patch installed successfully, and the total number of computers that need the patch. The audit should allow you to view by computer name where it lies in the patch deployment process. Being able to know who has the patch installed successfully and who does not can greatly improve your deployment time line. If you monitor your audits you will be able to see trends develop that can assist your next deployment procedure. The guidelines we just covered are just a few; there are many more that should be included in your company's patch management policy.

Once you have your patch management policy in place the next step is deciding how you are going to apply the patches. Microsoft gives you the options of using Windows Update, SUS Server (Software Update Services), and HFNetCHK Pro. These are some of the software packages approved by Microsoft.

Windows Update website is probably the best known way to install virus and security patches. Windows Update website is considered an extension of the Windows operating system. Windows update works with Windows 98, Windows 98 second edition, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advance Server, Windows Millennium, Windows XP home, Windows XP Professional, Windows Server 2003, and the 64 bit version of Windows 2003 server family. However, Windows Update website does not support Microsoft Exchange Server or Microsoft SQL Server. Since Windows Update can only be run on the local machine it has some limitations. By default the user must execute the install and since it relies solely on the user there is no guarantee the patch will be installed. You can change the setting to automatically download and install the patches but if this is done you will have patches install without testing. Changing the setting to automatically install the patches is not a good idea and can be detrimental to your company's network. Once you are ready to run Windows Update, you must first scan your computer. The scanning process examines the local computer to get details about what operating system you are running and what patches are currently installed. When the scanning process finishes, Windows Update gives you the ability to review each vulnerability patch that needs to be installed. Windows update also gives you the option to install critical updates, operating system specific updates, or device driver updates. The device driver option will allow you to download and install a driver on your computer that has been designed for the Windows operating system. Another feature of windows update is the ability to look at the installation history. This allows you to go back and check to see if a particular patch has been installed successfully. Since some updates require a reboot once they have completely installed using Windows Update can be time consuming,

Another tool offered by Microsoft is the Software Update Services or SUS server for short. Software Update Services has two parts the server side and the client side. The server side must have the Software Update Services software installed on a computer that is running a Windows 2000 server with service pack 3 and must have IIS installed. Since IIS must be running on the SUS server it would be extremely wise to make sure you are applying the latest IIS security patches. As mention earlier the SANS/FBI list IIS as the number one security vulnerability. The client side must have the SUS service running in order to perform properly. Software Update Services only works with Windows 2000 and Windows XP. This limits the ability to deploy the SUS in some company networks due to operating system limitations. There are still a tremendous amount of Windows 98 and Windows NT 4.0 computer networks still in service today.

The SUS server works by connecting to the Windows Update website and downloading the patches to your server. If you are using multiple SUS servers in your

network you can setup manually a content distribution point. This will allow other SUS servers the ability to receive the patches without having to go outside your company's network. Once these patches have been downloaded to all of your SUS servers you have the ability to decide which patches you want the clients to be able to install. Software Update Services has the ability to schedule install and service large corporate networks. While this type of deployment has its advantages there are some disadvantages. A major disadvantage is setting up. Depending on how your network is setup setting up the SUS server can be time consuming and difficult. Some of the issues I have seen have been the use of Group Policy and not having the ability to take care of all of your current computer's operating systems.

HFNetCHK Pro is a software package that was created by Shavlic Technologies and is based on HFNetChk.exe. HFNetCHK Pro software allows you to scan large computer networks and deploy patches from a central location. Major difference between Windows Update and HFNetCHK Pro is the fact that HFNetCHK Pro can scan for Exchange server vulnerabilities and SQL server vulnerabilities. This is a huge benefit HFNetCHK Pro uses a XML file to decide what patch to install on what system. Since HFNetCHK Pro is endorsed by Microsoft, it has some similarities to Microsoft Baseline Security Analyzer. They both use the same engine and the same database setup. The benefit of using the some of the same process allows HFNetCHK Pro to use the Microsoft Security Bulletin website to down load the latest patches. The fact that HFNetCHK Pro can apply patches on the following operating systems and application Windows NT 4.0, 2000, XP and Server 2003, Exchange Server, SQL Server, Microsoft Office including Outlook and Office installation points, Java Virtual Machine, Internet Explorer, Internet Information Services (IIS), Windows Media Player, Microsoft Data Access Components (MDAC), ISA Server, Commerce Server, and .NET Framework makes it one of the most versatile software patching programs. HFNetCHK Pro run on Windows 2000 with SP3 or higher, Windows XP, or Windows 2003 operating systems.

The main differences between HFNetCHK Pro solutions and Microsoft's Windows Update include:

- Low, Moderate and Important security updates - Windows Update focuses only on Critical security updates and does not typically cover Low, Moderate, or Important security updates from Microsoft. HFNetCHK Pro solutions cover all security updates, regardless of criticality rating.
- More products – HFNetCHK Pro solutions cover SQL Server (and MSDE), Exchange, ISA, NT4, and Office detection. Windows Update does not.

- Non-security updates and drivers – Windows Update includes Microsoft non-security updates and drivers. Shavlik's solutions cover security updates only.
- Agents – Shavlik's HFNetCHK Pro solutions do not require that an agent be installed on target machines, but Windows Update does. Agent less patch management means simplified rollout and increased awareness of rogue machines on your network.[6]

These key features set HFNetCHK Pro apart from other patching software. HFNetCHK Pro can be installed and push patches within minutes. This feature alone can be critical when a new virus has been detected. HFNetCHK Pro utilizes XML data files that are updated the moment a security patch is released. Since HFNetCHK Pro works directly with Windows Update your patches will always be up to date. No need to install agent software on the machines being scanned. Only those patches that are necessary and applicable to the scanned platform are evaluated during the scan process. Unnecessary and superseded patches are not presented if they are not needed. This is feature is extremely important because Microsoft has started releasing security rollup patches. These patches are created to fix multiple security vulnerabilities with one patch install. HFNetCHK Pro checks the registry, the file version and the checksums for each patch installed. HFNetCHK Pro is built upon the same engine that powers the Microsoft Baseline Security Analyzer and the SMS Feature Pack and is driven by the same database schema used by the Microsoft Security Bulletin website.

I am responsible for patch management at my company. My responsibilities cover two states with 1,500 + machines. We currently use a combination of all the patching products talked about earlier. HFNetCHK Pro has been one of the easiest software patching tools I have used to date. Crossing different domains and local administrator permissions have been the only two issues I have seen so far. In 10 weeks we went from 43 percent of our computers being vulnerable to viruses or security vulnerabilities to 0.01 percent vulnerable. HFNetCHK Pro made this all possible.

[6] **HFNetChkPro4**
http://hfnetchk.shavlik.com/onlinehelp.asp

Summary

With the speed a viruses or security vulnerabilities can infect your network it is important to realize the importance of patch management. While there are many aspects to a patch management policy it is important to at least cover the basics. Deciding on which deployment tool to use at your company will depend largely on the size of your company. Since HFNetCHK Pro was designed in cooperation with Microsoft, in my opinion HFNetCHK Pro is the best choice for software to deploy security patches. A patch management policy and program should be an asset to your IT department not a burden.

REFERENCES:

Virus Primer
http://www.trendmicro.com/en/security/general/virus/overview.htm

In need of a quick fix
http://www.fcw.com/fcw/articles/2003/1201/cov-patch-12-01-03.asp

Spending To Fend Off Online Attacks Grows In 2004
http://www.informationweek.com/story/showArticle.jhtml?articleID=17100128

Labs Answers Patch Management Questions
http://www.eweek.com/article2/0%2C4149%2C1257572%2C00.asp

Patch Management Strategy Announcement
http://www.myitforum.com/articles/5/view.asp?id=5253

'LovSan' Worm Crawls Into Philly's City Hall
http://www.nbc10.com/technology/2400607/detail.html

Patch management best practices
http://www.fcw.com/fcw/articles/2003/1201/cov-patch2-12-01-03.asp

Keeping up with patch work near impossible
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci796744,00.html

The vicious circle of patch management
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci941967,00.html

General Information Security Statistics:
http://www.securitystats.com/infosec.html

http://www.securitystats.com

How much do computer virus attacks really cost?
http://slashdot.org/askslashdot/01/02/07/2354227.shtml

Hackers and viruses to cost business $1.6tn
http://www.vnunet.com/News/1106282

Viruses Cost Big Bucks
http://www.wired.com/news/technology/0%2C1282%2C20297%2C00.html

"Code Red" Worm Strikes 115,000 Internet Servers
http://pcmag.com/print_article/0,3048,a=10839,00.asp

The Most Destructive Viruses of All Time
http://technewsworld.com/perl/story/32422.html

SANS/FBI releases latest top 10 Linux/UNIX vulnerabilities
http://asia.cnet.com/itmanager/trends/0,39006409,39156753,00.htm

Reducing Internet-Based Intrusions: Effective Security Patch Management
http://csdl.computer.org/comp/mags/so/2003/01/s1050abs.htm

Microsoft Windows Update
http://v4.windowsupdate.microsoft.com/en/default.asp

Deploying Microsoft Software Update Services
http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

HFNetChkPro4
http://hfnetchk.shavlik.com/onlinehelp.asp

Cert/CC Statistics 1988-2003
http://www.cert.org/stats/cert_stats.html

General Information Security Statistics:
http://www.securitystats.com/infosec.html