Global Information Assurance Certification Paper

Areas to Consider When Planning Virus and Software Updates of Remote Computers

By J.J. (Jeff) Markee
January 15th, 2002
GSEC Practical - Ver 1.3

Executive Summary:

Hackers and virus writers utilize known vulnerabilities to compromise systems and spread their payload. Therefore, keeping software patches and anti-virus pattern files up-to-date on remote computers is essential to a corporate-wide "defense-in-depth" approach for IT security. Often remote computers are forgotten in the list of what to patch, since they are not "on the network". With broadband connections increasing in number, these computers are quickly becoming a direct extension of the corporate network. These remote computers are a risk and require the creation of specific policies and procedures to allow for the smooth distribution of software patches and anti-virus updates.

This process should be as automated as possible and controlled by IT. Remote users should **not** be responsible for selection or installation of software patches and virus software updates. This will ensure that the entire corporation is consistently receiving the appropriate software patches and virus updates to ensure "defense-in-depth".

Focus of the Paper:

Hackers and virus writers utilize known vulnerabilities to compromise systems and spread their payload. Therefore, keeping software patches and anti-virus pattern files up-to-date on remote computers is essential to a true corporate-wide "defense-in-depth" approach for IT security.

A difficult problem for global companies is keeping mobile computers updated with patches and virus software. This paper will focus primarily on remote users, including sales force and home office employees. These users spend 100% of the time outside of the office and both collect and distribute vital data. Maintaining current patches and virus software on all computers including remote computers is the ultimate goal for IT security. Achieving this goal creates a secure platform with which corporate activities can take place.

This paper will focus on issues that need to be thought through and documented, to assure the proper policies and procedures are in place for effective distribution of patches and software updates to remote computers.

"Above all, enterprises should establish processes to make sure they promptly apply all security patches to all Internet-exposed systems"[1]

Assumptions:

The following assumptions are being made for this paper:

- Corporate standards are Microsoft centric software installations

- Remote connections are established securely, through VPN connections
- Two-factor authentication and strong passwords are used for authentication
- Servers that are being accessed by remote computers are in a secure DMZ behind a firewall and not part of the corporate network:
  - Limits will be placed on specific IP's remote computers are allowed to access.
  - Intrusion Detection Sensors will be behind the firewall and on the servers of access
  - Virus scanning on the mail stores of remote mail servers.
- Laptop and home desktop configurations will be standardized across the corporation and should be maintained at the same level of currency as the LAN connected personal computers on the corporate LAN.
- All remote computers should be corporate owned assets to avoid any licensing configuration issues that may arise from using an employee's personal computer.
- An up to date personal firewall software protecting broadband / always on connections (this also should be maintained by IT)
- Remote users are not part of IT and do not understand computers. Think of your worst sales force user, this one person is the weakest link that needs to be patched.
- All patches need to be applied by IT. If users begin applying patches this creates versioning and support issues for the standard hardware and software builds.

In order to ensure security both software patches and virus software must be kept up-to-date. Remote computers need to be maintained by corporate policies and guidelines. Remote computers will be a greatest risk for theft, and may be subjected to hostile network environments while on the road. Remote computers use guest accounts in other company networks, hotels and at home. The maintenance of remote computers and needs to be centralized, and cannot dependent on the sales force user.

Classification of Users

Every company has several different classifications of users. These users are

- Office Only (Never Remote) – These users are administrative staff, and factory/ production control personnel. They use standard desktop computers that will physically remain on the company's premises. These computers will always get access through a NIC card and should not have a modem installed.
- Mixed – LAN and Remote – These users will use laptops that can either be connected directly to the LAN or remotely from home via a modem (cable, ISDN, or analog) or guest account on another LAN.
- Remote – These users are removed physically from the company and can be connected through a modem (cable, ISDN, or analog) or guest account on another LAN. These employees include roaming sales force and home office personnel.

Areas of consideration

There are many things that should be considered when designing how to keep remote access computers current and secure. This paper will focus on several areas of considerations for maintaining patch levels and anti-virus software on remote computers:

- Creation of Policy
- At what connection speed will remote computers attach to the corporate network?

- What is the frequency and duration of remote connections?
- What is the process for updating the remote computers?

The issues with remote users are:

- Maintaining application and operating system software updates (security and functionality patches)
- Updating virus software
- Software inventorying (limited SMS capabilities)
- Secure access and transfer of corporate data (sales information, contact tracking, marketing collateral)
- Secure access to e-mail

Microsoft's Security:

Most current corporate system configurations are Windows-based. Hackers and virus writers will continue to design exploits for this platform since it has the largest install base. Microsoft has stated a firm commitment to better security but with the release of Windows XP, a new security hole was discovered that impacts:

- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows XP

Microsoft has released a critical update for this vulnerability. The Microsoft MS01-059 bulletin can be found at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp[ii]

"Measured by the number of security bulletins the company has released, Microsoft's progress in security is mixed. In 1999, the company issued 60 security advisories, followed by a whopping 100 in 2000. That fell back to 60 last year."[iii]

This means that there were 60 patches that could have been applied to different Microsoft products. While many of these were server patches, there are a large number of patches that may need to be applied to all computers within an enterprise.

Additionally during the second week of January, 2002 a theoretical virus was distributed to anti-virus software vendors, to demonstrate a security hole in Microsoft's .NET intermediate Language (MSIL). [iv] This is the direction with which the Microsoft platform is heading with the assurances from Microsoft that this will be a secure platform.

Even though many prior exploits have gone against Microsoft's IIS web server, future versions of Microsoft's operating system will have both IIS and Internet Explorer embedded in their code.[v] This brings future risks into the native OS, which increases risk of infection from the number of machines from have FrontPage or IIS running to all computers running Windows 2000 and XP.

A list of all of the Microsoft Security Bulletins can be found at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp [vi]

Hypothetical Example of Risk:

When remote users have broadband connections to the network they become and extension of the network. If these computers are not up to date with software patches and virus software they are a risk to the entire network.

The following is an example of the risk a remote computer can pose to a corporate network. A home office worker with a broadband connection goes to a Microsoft Hotmail account. This remote computer has not been kept up to date with patches or with virus software. The user downloads an attachment from a Hotmail account, which is infected with Nimda, Goner or the current virus of the day. The virus begins replicating in the personal address book, which begins sending thousands of messages to the corporate Exchange server. This traffic quickly can overload many Exchange servers causing a mail denial of service attack. Also this infected machine can serve as a launching point for additional infections throughout the enterprise, or as a zombie machine for a hacker to utilize.

Real World Example:

"After Microsoft acknowledged on 25 October 2000 that a hacker penetrated its corporate network, news reports indicated that the attack may have originated from an Microsoft employee's or contract worker's home PC. Moreover, according to news reports, the PC used in the attack was said to have been infected with malicious software that allowed the hacker to log in remotely to Microsoft's networks."[vii]

Creation of Policy:

The first place to start is with the authorization and clarifications of how, why and when updates will be sent to users. This policy needs to outline for users what is expected of them, and give them a clear understanding of why these things need to be done. This policy needs to be approved by all interested parties to make sure that constraints are "livable" for the end users. The policy needs to outline the following for remote users.

- Times of Connections / Access:
  - Are connections available 24 by 7 by 365? Most companies require always up connections, however IT needs to have scheduled maintenance times, where the service may not be available. The longer this is on the calendar the easier it is to have an outage during the scheduled time.
  - Will there be a standard maintenance schedule? Times that remote users need to be aware of, because remote resources will not be available?
- Upgrades and Patch Schedule:
  - What is the release schedule for patches?
  - A scheduled release needs to be created to prepare users that updates can be applied. The release schedule should be the same day every week. If there is a release day that updates come out on remote users will know this and plan for the updates.
- What updates will be available?

    - Not all patches need to be applied all the time. If a patch has no relevance to the remote PC then this will not be applied.
    - Testing of patches needs to be done prior to release within the network. Each patch should be tested to make sure it does not break or create conflicts with other previously installed software.
- Updates to Virus Software:
    - Updates to virus software should be pushed out as soon as they become available.
    - This can depend on your means of distribution for Pattern or DAT files. Unfortunately some Antivirus software configurations do not allow for incremental updates and entire pattern files need to be sent the users. In these cases a twice a week schedule should be established.
- Delay of patch application, and X day Rule:
    - The ability to delay a patch or pattern update is necessary for sales forces since there are times when a 30 minute connection to the home network is not available. The allowable time of delay will vary from company to company.
    - The X day rule will be activated if users continue to delay patch application. After a certain number of days patches will be forced on the user irregardless of their connection speed. Again this varies from company to company.
    - Both these policies need to be clearly stated for the remote users understanding and acceptance.
- Connection Speeds:
    - If a user is connecting below a corporate determined speed threshold (i.e. 10 Kbps) then they will not receive the update unless they have exceeded the X day rule above.
- Responsibilities:
    - What are IT's responsibilities? Clearly state what actions IT will perform and when these actions will take place. Give contact information so that users have a place to call for assistance.
    - What are the users responsibilities? Clearly state any actions that the user will be required to perform. The patch application should be an automated process without requiring user intervention.
    - Do remote users need to connect once a week? Is there are time frame that users are required to connect within? Some sales databases require nightly connections while others are completely autonomous and never need to synchronize. This will very from company to company.
    - Do users need to accept patches? Allowing for remote users to accept patches allows users to feel as if they have some input and control over the updating process. This again will vary from company to company. Some companies will choose to do everything in the background, while other will want to include the remote user in the update process.
- Internet Use Policies – What is acceptable Internet use by employees? The SANS reading room has several papers that address this issue. Two recommended are:
    - "Managing Internet Use: Big Brother or Due Diligence?" by Steve Greenham URL: http://rr.sans.org/policy/internet_use.php [viii]
    - "Acceptable Use Policy Document" by Raymond Iandolo URL: http://rr.sans.org/policy/accept_use.php[ix]

At what connection speed will users be connection to the corporate network?

There are many different methods for remote users to connect back to the corporate network. These connection options include:

- Wireless Phone
- Dial-up
- ISDN
- Broadband
    - DSL
    - Cable
    - Satellite

While the size of downloadable software patches continues to grow rapidly, many connection speeds cannot efficiently handle the amount of data for the patch. This inability to download at an efficient rate affects many remote users. For example, sales forces are mobile and can travel up to 50% of the time. Because of their schedule, they require several methods for connecting to the corporate LAN. Even if remote users have a broadband connection in their home, there will be many times when a dial-up at a hotel will be the only method available for getting updates. Therefore, downloading patches and updates can become burdensome to dial-up users and these users need to be considered in the overall updating process.

Dial-up limitations:

In many rural areas within the US, the Internet access is slow due to the use older phone switching equipment. In addition, the connection speed will include many developing countries where Internet access is established with antiquated phone lines and encounters frequent interruptions.

It is imperative that the IT personnel understand at what speed the remote user is connected each time. If the connection speed is greater that X Kbps then patches can be sent. However if the remote computer is on a poor connection or is connected by a single channel cell phone at 9.6 Kbps then updates should not be sent. A suggested test is to examine the connection speed against the minimum baseline. If the connection speed is greater than the minimum, then the patches can be sent as long as the user has accepted them.

The risk in the above scenario is that if remote computers continually connect over slow-speed connections, then they will never receive updates. This is where the (X) day rule becomes in effect. If a user is more than (X) days behind on patches or virus pattern files, they will have the patch or virus pattern forced upon them no matter what connection speed is established. In order to achieve this activity, the corporation must have the appropriate policies in place to support such a forced download of large files.

Risks with Slow Connections:

When remote users are limited to slower connections, large patches can add lengthy delays to the connection process for the remote users. This is viewed as unproductive time and can reflect negatively on the IT organization if not handled with care. The possibility of a lost sale from a

sales person trying to connect to the network to get a specific file and then being required to download a large patch is unacceptable. This is why the policy of allowing for a delay before downloading the patch is suggested.

Many sales forces are still constrained by limited access to broadband connections. Corporate solutions need to be designed with an appreciation of slowest connections, and an understanding that not everyone can connect at T-1 speeds.

Risks with Broadband Connections:

Too Much Bandwidth:
Along with the always-on risk of broadband connections there is also a risk of too much bandwidth coming into a company. If there are many remote, and home office users with broadband connections, the bandwidth for the remote access firewall could be saturated very quickly. Specific software (such as Floodgate-1™ by Checkpoint) can restrict the amount of bandwidth that is utilized by specific connections and make sure proper traffic control is maintained for remote users. This type of software can limit the amount of bandwidth allocated to broadband users. This will mean that broadband customers will not fully utilize their capabilities, but will allow for more simultaneous connections. Additional information on Floodgate-1 can be found at
http://www.checkpoint.com/products/performance/datasheets/floodgate-1_datasheet.pdf [x]

Limited Access Points:
Broadband is not the cure all for updating remote computers. Broadband is still limited to urban areas.

"About 10 percent of U.S. homes get broadband, up from almost none in 1998. Historically, this rate of adoption compares favorably with other new consumer electronics products. Getting to 10 percent household penetration took 12 years for color TVs, eight years for cell phones and four and a half years for CD players, according to figures compiled by the Federal Communications Commission. But broadband hasn't lived up to the hype."[xi]

The investment has been made in the main infrastructure for broadband, but the last mile is where the connections need to be made.

"The story of broadband is one of arrested development. In the last decade, investors plowed $90 billion into the construction of a cross-continental fiber-optic broadband network. Today, a mere 3 percent of that backbone is in use. The other 97 percent remains dark because only 10 percent of homes and smaller businesses are connected to it. The rest await access but have been frustrated by the cost and difficulty of upgrading the local telephone networks"[xii]

Broadband is the future in the US, however sales forces in developing countries and the rural US do not currently have this option for fast Internet access. If you are supporting global operations you cannot forget that, everyone does not live in New York, and broadband is a promise for the future, but users need support today.

What are the Frequency and Duration of Remote Connections?

Frequency

Some remote users will connect to the corporate network five or six times a day, while others will synchronize once a week. The assumption can be made that the majority of remote users will synchronize once or twice a day.

The more frequently the user connects, the less data that will need to be synchronized with each connection.

Duration

The duration of the connections to the home network is a function of speed of connection and amount of data that needs to be transferred.

Duration of connection to Corporate Network = (Amount of data transferred) x (Speed of connection)

There are many applications that need to send or receive data from the corporate network. All of the data transfer needs of these different applications must be recognized to create the average amount of data for downloads.

- What is the e-mail system that is used?
    - E-mail systems vary the amount of data they send back and forth, some are chattier than others. Additionally, it is important to understand what type of data the remote users are sending or receiving. If remotes users are sending simple text messages versus graphical presentations this will affect the amount of time that the remote user will need to be connected to the corporate network.
- Are there sales databases that need to be updated?
    - How is sales information updated?
    - Is there a need for nightly synchronization?
    - Is this a batch process that requires multiple connections?
    - Is the sales data independent for each sales representative?
- Are there expense databases that need to be updated?
    - Does expense traffic go through a separate application?
    - Will expenses be approved through digital signatures?
- How much contact and marketing information needs synchronization?
    - How does the sales representative get lead sheets and/or new perspective clients in their sales area?
- Are there file share areas that the user needs to access?
    - Is there information from the corporate sales force Intranet site that is important for the sales team to read?
    - Are marketing materials stored electronically on a sales force share area?
- How are anti-virus software pattern/DAT files and virus engines be updated?
    - Are pattern files done incrementally?
    - Do anti-virus files require a full download of patter / DAT files?
- What personal firewall software is being used?

- Inventory software
    - Is a periodic software check being run to check for changes in software installations?

Once all application data transactions are understood, an estimate of the duration of calls can be created and an estimate of the impact of patches can be explained to the remote users.

What is the Process for Updating Remote Computers?

Updates should be sent to the user though the remote user login mechanism, e-mail synchronization process, or through expense tracking software. Updates should occur in the background, if possible.

Testing of patches needs to be done prior to release within the network. Each patch should be tested to make sure it does not break or create conflicts with other previously installed software. Once patches are tested they need to be approved and staged for the rollout of the patch(s) to the different computers.

A process needs to be established that removes as much human interactivity as possible. This means that if there are two buttons required for updating there is one button too many. Users should simply have to answer "yes" or "no" to the updating mechanism.

Detailed hardware and software inventories need to be kept to make sure that all known configurations are documented and that the patch levels can be tracked. If a software patch does create a conflict, a study needs to be done to explain the alternatives that management will have to either resolve the conflict of live with the risk of the unpatched system. Resolving these conflicts and having the patch installed should be recommended approach.

Detailed records need to be kept to make sure that all computers are being updated appropriately. If a computer is not being updated and is connecting to the corporate network, it becomes a bigger and bigger risk to the corporate network as time goes forward.

Schedule the Updates:

Schedules are a good thing; they allow everyone to know what and when to expect changes. Update schedules should:

- Be well known – this is done by having the same schedule for a long period of time, and reminding people of the schedule often. This consistent day of when updates will be distributed in order to allow the sales force to prepare to have a longer connection.
- Maintained even if no updates are necessary the schedule should be the same and publish the fact that no updates are necessary.
- A list of changes to expect should be published prior to rollout.
- Users should also be allowed to have some say in when updates are sent to their machine. This configuration should be similar to password update notifications. Users should be allowed to delay updates until a convenient time. This means that users should be able to decline updates for up to XX hours (time frame for enforcement is subjective, but there needs to be a time limit). Otherwise users would continue to delay updates continuously.

User must also be aware of the X day rule, in which updates will be forced on them after a specific number of days.

Schedule Example:

For example, the scheduled day for updates is every Wednesday's and there is a 72-hour delay maximum. If a sales person has a presentation on Wednesday, he or she already knows that they must schedule some time for an update sometime during the next 3 days. Otherwise he or she will know a forced update will occur irregardless of their response or connection speed on the 4th day.

Alternatives to Over the Wire Updates:

With corporate assets and data going into many locations around the world, is a 28.8 Kbps connection sufficient for today's e-mail delivery, sales data synchronization, and anti-virus updates?

Alternatives to over the wire updates are to send media kits, CDs, to remote users for self-updating. This requires:

- Creating and testing the CD configurations
- Physically sending a CD and verifying receipt
- Knowing mailing addresses for all remote users and computers
- Some action must be to be taken by the end user once CD is received. (Inserting the CD into the machine).
- These updates then must be scripted to automatically loaded onto the remote computer.
- Additional budget, to pay for the extra costs of creating and mailing CD's to the remote users, must be obtained.

Even if the process for creating the CD's is 1 week, the distribution and installation of the patches and updates can be delayed by a few weeks. This means from a patch stand point users can be at best 1 month if not more out of date, and that is a risk.

Additionally many companies do not want to incur the costs of monthly mailings. These companies will send out CD's quarterly, semi-annually, or annually to save cost, but this increase the risk. While the distribution of CD is not the preferred method of distribution, it cannot be ruled out as a possibility for some companies.

Conclusion:

While remote computers are not directly connected to LANs, these machines represent a risk to the corporation and cannot be forgotten. With broadband connections increasing in number, these computers will be a direct extension of the corporate network. A policy and strategy for keeping remote computers updated needs to be created and enforced. This strategy must balance functionality of the large bandwidth remote computers with the limitations of slower analog connections.

This process should be as automated as possible and controlled by IT. Remote users should not be responsible for selection or installation of software patches and virus software updates. This

will ensure that the entire corporation is consistently receiving the appropriate software patches and virus updates to ensure "defense-in-depth".

References:

[i] Gartner.com, August 1, 2001, "Lack of Security Processes Keeps Sending Enterprises to 'Code Red'", by John Pescatore, Gartner FirstTake, FT-14-2441

[ii] Microsoft Security Bulletin MS01-059 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp

[iii] CNET News.com, January 11, 2002 "Microsoft's security push lacks oomph", by Robert Lemos URL: http://news.cnet.com/news/0-1003-200-8437230.html

[iv] CNET News.com, January 11, 2002 "Microsoft's security push lacks oomph", by Robert Lemos URL: http://news.cnet.com/news/0-1003-200-8437230.html

[v] Gartner.com, September 19, 2001, "Nimda Worm Shows You Can't Always Patch Fast Enough", by John Pescatore, Gartner FirstTake, FT-14-5524

[vi] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

[vii] Gartner.com, November 2, 2000, "Home PCs Are the Weak Link in Enterprise Network Security", by John Girard, John Pescatore, Gartner FirstTake, FT-12-5300

[viii] "Managing Internet Use: Big Brother or Due Diligence?" by Steve Greenham URL: http://rr.sans.org/policy/internet_use.php

[ix] "Acceptable Use Policy Document" by Raymond Iandolo URL: http://rr.sans.org/policy/accept_use.php

[x] Checkpoint's FloodGate-1 software data sheet URL: http://www.checkpoint.com/products/performance/datasheets/floodgate-1_datasheet.pdf

[xi] The Washington Post, Dec 12, 2001 pA35 "Broadband's Faded Promise" (Editorial) Robert J. Samuelson.

[xii] The New York Times, Dec 10, 2001 pA21(L) col 02 (17 col in), "The Broadband Economy". (Editorial Desk)(Op-Ed) Karen Kornbluh