Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Issues with Keeping AntiVirus Software Up to Date

Exploring different aspects of keeping ANY virus protection software up to date to be protected from virus infection. It is obvious that as Information Security professionals that we need to be aware of all of the "latest and greatest" information on outbreaks of malicious code, including how to recognize and repair them. Also, we know that we need to have virus protection software loaded at all possible points of failure within our organizations and we need to have procedures for when these outbreaks occur. However, o...

Copyright SANS Institute
Author Retains Full Rights

AD

John Graham
Assignment version 1.2e

Issues with keeping AntiVirus software up to date

Purpose:

Explore different aspects to keeping ANY virus protection software up to date to be protected from virus infection. It is obvious that as Information Security professionals that we need to be aware of all of the "latest and greatest" information on outbreaks of malicious code, including how to recognize and repair them. Also, we know that we need to have virus protection software loaded at all possible points of failure within our organizations and we need to have procedures for when these outbreaks occur. However, it seems to me that one of the most difficult tasks is keeping all of this virus protection software up to date. All reputable virus protection software products come out with updates on a fairly frequent basis, and it is up to each organization to get these updates out to all computers that need to be protected. There are many ways to do this and many challenges that we face in accomplishing this, but it is important to keep our organizations as "clean" as possible.

Specific topics included in this paper:

1. Why it is so important to be able to keep your virus protection software updated, especially in a major outbreak situation

2. Challenges that we face with keeping this software up to date with possible solutions

3. What products are available that can help with keeping your virus protection software up to date

Why it is important to keep your virus protection software up to date:

Malicious code creators are constantly at work trying to accomplish various things through their "work". Whatever the goal, we need to do whatever we can to protect ourselves before these things penetrate our environments. While they are doing their thing, virus protection software companies have their experts trying to sniff out this code and make it so that their software can detect and clean it. Having virus protection software installed at all vulnerable points in our networks (typically, this is email, file servers, and user workstations) is the first step, but having well defined procedures to keep this software up to date against the latest malicious code is the next step.

A good example of this can be found in an article on the "civic.com" web site (http://www.civic.com/civic/articles/1999/CIVIC_050399_41.asp) from May of 1999 referring to Portland, Oregon's problem with the Melissa virus. "Fortunately, an estimated nine of out every 10 desktop systems now include anti-virus software, which detects and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

removes such unwelcome code. However, it's important to note that installing anti-virus software is only a first step in keeping systems clean. Hackers constantly tweak existing viruses or develop new ones, and that means network administrators need to be just as clever in guarding against viruses by downloading anti-virus packages early and often". This is from more than 2 years ago, but is still a good example of the need to keep virus protection software up to date including procedures for "hustling" these updates out in major outbreak situations like Melissa.

On the Maine School and Library Network web site (1 below in references) they suggest that you update your virus protection software at least once a month, but that as often as your AV software vendor comes out with updates is even better. It is also important to look at the various systems you need to cover and decide how best to get them the updates. Are they on a local area network or not? Do they have direct internet access or not? Will the machine be used to receive email directly (as opposed to through a protected server)? Answers to these types of questions can help you decide how and when to get updates to your systems.

Our company recently used our "in-progress" procedures for emergency virus protection updates to protect us from the emerging W32/SirCam@MM virus. We quickly updated our email protection and made the update available for our end user workstations in a short amount of time and we did not take any kind of substantial hit. This was the case even though our email system showed us we received hundreds of these emails (i.e. if we had not updated our virus protection software in short order, we could have had a major infection in our company).

Challenges that we face with keeping this software up to date with possible solutions:

Most organizations of any size have computer systems that can be accessed in a number of ways. Workstations can be connected via a Local Area Network, a broadband connection like DSL or Cable Modem, dial-up analog phone line, or the Internet. Typically, these systems have some sort of data that is valuable to the organization and needs to be protected from virus infection. Having systems connected in so many ways can make it difficult to keep them updated on a regular and emergency need basis. Below are some common examples of difficult update situations and some possible solutions to them.

1. **The "road warrior"** – These are users that are often away from the corporate network with a laptop PC that they use to connect via analog dial-in to the corporate network directly or to the Internet and then into the corporate network through VPN. More than likely they had virus protection software loaded when they originally received the machine, but it is a unique challenge to keep them updated, for a number of reasons.

   =) If they connect directly to the corporate office via dial-in, you often do not know

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

how often and when they may be connecting, so it is difficult to schedule an AV product to update from your corporate network at a time when they will actually be connected.

=) Some of these users do not dial-in much at all to the corporate network, which obviously makes it difficult to update them from there, but they may vulnerable to virus infection from other sources and could infect your network when they do connect.

=) Having users physically away from the corporate network is harder to support than machines that are actually located where the corporate LAN is.

Two possible solutions for these situations:

=) Many virus protection vendors offer ways to update directly from the Internet. If your "road warriors" typically have Internet access, that is a good option.

=) At our company we have set the AV software to update from a location on the machines hard drive and have given the users a couple of ways to actually download the updates to the proper location on their machines hard drive where it can update from.

2. **Systems on remote networks from the "main" corporate network** – these are systems that are physically located away from the corporate network, but are connected via some sort of WAN connection (DSL, Frame Relay, T1, etc…). Hopefully they are connected in a way to get updates from the "main" corporate network, but things like subnetting on remote networks and the way your virus protection software is able to do updates can make this difficult to accomplish. Also, as with the "road warriors" above, having these systems physically located far away can make it difficult to monitor whether they are getting updates or not and just supporting them in general.

   Some options for these situations:

   =) If possible, designate a qualified "site coordinator" for getting updates to their LAN on a regular basis and making sure machines on that network are set to properly get updates from the LAN (as well as other possible responsibilities).

   =) If the remote office has some sort of direct connection to the Internet, they could get updates that way from most virus protection software.

   =) Assuming they are on the corporate email system, you could automate a process to send updates via email to these users.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3. Lackadaisical or uninformed Users – These are people that for whatever reason do not feel that keeping their virus protection software up to date is important or is just too difficult and time consuming to do. It is always best to automate things like software updates of any kind so that little, if any, user intervention is needed, but sometimes there is no choice but to have the users responsible in some way for performing updates.

   Some options for these situations:

   =) Have it clearly stated in an Information Security Policy what their responsibilities are in terms of keeping virus protection software up to date.

   =) Continuous education via Intranets, newsletters, and other forms of communication on how important it is to stay updated with real examples of virus threats in the wild that could impact them.

   =) Make training available when they get their computers so they feel comfortable from the get go.

All in all, these and other situations make keeping your systems virus protection software up to date an unenviable task, but with persistence, planning, and patience, you can protect your organization from virus infection.

What products are available that can help with keeping your virus protection software up to date:

There are many anti-virus software companies out there any many of them have excellent tools to assist with keeping your system's virus protection software up to date. These range from simply having "point products" that can be set to update from somewhere on a scheduled basis, to full-fledged management products that help you get updates out fast in emergency situations. A quote from the book, Mastering Network Security, is relevant here. "A scaleable virus protection solution will not only reduce overall costs, it will help to insure that your environment remains well protected. As mentioned, virus-scanning vendors periodically release updated signature files. These signature files are of little use, however, in they are not installed on every system that requires them." Below are some examples of these products and their various features.

1. **Network Associates McAfee E-Policy Orchestrator (EPO) version 2.0** – This is a powerful management tool that helps you manage your updates, as well as other things, for most of McAfee's virus protection point products. Examples of the point products include NetShield for NT and 2000 Server and VirusScan multiplatform version 4.5 for Windows 9x, NT, and 2000 workstation. From a central console you

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

can initiate updates on some or all of your machines that have the EPO agent installed on a regular schedule and/or an emergency on-demand basis. Some specific ways EPO can help with updating virus protection software:

=) "Agent wakeup call" – Each machine that has the EPO agent is set to communicate with the EPO server at a specified interval to get updates. This includes tasks that can be created to have the point product update in some way. If there is an emergency situation where you want to get clients updated as soon as possible, you can send this "agent wakeup call" for the client to check the server for new tasks and so forth and do an update immediately.

=) "Task on Connection" – For remote users who dial-in via analog phone line, this option to do updates can be very helpful. You can create an update task that is scheduled to run "on connection", which means that the EPO agent knows when a connection is established and will run a task then, as opposed to some scheduled time when the computer may NOT be dialed in.

=) Powerful reporting capabilities that can show you what machines are NOT receiving updates so you can investigate why.

For more information on this product, go to the following web link:

http://www.mcafeeb2b.com/products/epolicy/default.asp

2. **Computer Associates eTrust AntiVirus** – This is the latest virus protection product from Computer Associates to manage your organizations anti-virus efforts. It has many of the same features that McAfee's EPO product has, including the following things.

   =) "Auto Signature Download" – this feature automatically distributes CA's AV "signature" files to all machines registered within eTrust on both regular and emergency on-demand updating situations.

   =) Powerful reporting capabilities that can show you what machines are NOT receiving updates so you can investigate why.

   For more information on this product, go to the following web link:

   http://www3.ca.com/Solutions/Product.asp?ID=156

3. **Symantec's Norton AntiVirus Corporate Edition version 7.5** - This is the latest virus protection product from Symantec to manage your organizations anti-virus efforts. It also has many of the same features that McAfee's EPO product has, including the following things.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

=) “Centralized management from a single console allows IT managers to lock down policies that keep systems up to date and properly configured, fully protecting users at all times”.

=) “NAVEX, a single, extensible scanning and repair engine, provides the unique ability to update virus definitions and engine extensions — without having to reboot servers or re-deploy application software”.

The above quotes are from the Symantec web site; further information can be found at the following web link:

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=23&PID=7352577

There are other products available that do similar things, but these are 3 of the industry leaders.

Summary:

While there are many factors to protecting an organization from virus infection, one of the most difficult is keeping virus protection software up to date on both a regular and emergency basis. New malicious code is created every day, which underscores the importance of keeping your protection up to date and having procedures to react to major outbreaks. There are many different products that offer different ways to keep their software updated, but it is up to each individual organization to come up with a plan to suit their particular environment. It is clear with new viruses coming out all the time that this will continue to be a challenge for Information Security professionals.

References:

1. Maine School and Library Network web site

   http://www.msln.maine.edu/circ_rider/virdef.htm

2. Network Associates McAfee business to business web site

   http://www.mcafeeb2b.com/products/epolicy/default.asp

3. Symantec web site

   http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=23&PID=7352577

4. Computer Associates web site

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www3.ca.com/Solutions/Product.asp?ID=156

5. Civic.com web site

http://www.civic.com/civic/articles/1999/CIVIC_050399_41.asp

6. The Book "Mastering Network Security", by Chris Brenton; page 374

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**