Antivirus Best Practices

A Net Sense White Paper

By Greg Reynolds

Consultant

(919) 870-8889
(800) 642-8360

Antivirus Best Practices

by Greg Reynolds

A virus outbreak on your network creates chaos and bleeds cash. In 2003, corporate giants such as Bank of America, First Energy, and Verizon were hit hard by preventable virus outbreaks.

Want to make sure that you're not next?

Here's what you need to do:

1) - Use a spam appliance at your internet gateway to block incoming spam.

The vast majority of viruses are spread by unwanted email, i.e. spam. Using a spam appliance stops 95% of all spam and prevents it from even entering your network.

Avoid the primary source of contamination and treat it like the plague that it is. Do everything you can to keep spam from coming into contact with your servers and workstations, including running a secondary spam filter on your mail server.

2) - Use two antivirus scanning engines against incoming mail.

Redundancy is a best practice in many fields and antivirus protection is no exception. No single antivirus solution is perfect at catching every virus. Your primary defense should be at the SMTP gateway before viruses reach a server.

Investigate, select, and implement a secondary antivirus solution that fits your budget and provides an extra layer of protection at the server level. You'll be pleasantly surprised by what the safety net catches.

3) - Update all antivirus signature files automatically every day.

Antivirus vendors create updated signature files for their detection engines when new virus threats are detected. Unless your system has the updated files in operation, you are defenseless against the latest and greatest viruses.

Make sure that your systems are setup to receive these updates automatically instead of upon administrator request. If your antivirus solution doesn't have automatic updating, start shopping for one that does.

4) - Publish and implement on your perimeter SMTP gateway and mail servers a list of forbidden attachments - .vbs, .pif, .scr, .bat, .cmd, .exe, etc. - and strip those out.

Dangerous attachments have no business entering your system at all. Even if they aren't blocked by your antivirus software, you should filter these types of dangerous attachments from all incoming and outbound mail.

If necessary, you can setup a "holding area" for stripped attachments that may contain desirable content (ex: .exe files) and implement a manual retrieve/review process within the IT department.

5) - Use antivirus software on every workstation and scan all outbound mail.

Viruses, trojans, and other malware can (and will eventually) enter your network at the workstation level. An end user can easily introduce viruses to a corporate network in a variety of ways including floppy, CD-ROM, external POP3 or IMAP4 mail servers, USENET newsgroups, instant messaging clients, Web mail, or email from an Exchange server.

Viruses and worms that can enter a network through mobile devices or PDAs have already been discovered and future malware of this class will only be worse. Make sure that all outbound mail is virus scanned at the workstation level as well as scanned again at the mail server.

6) - Set antivirus software to always scan all removable media, i.e floppy disks.

Don't let viruses in through the end user backdoor. Set your workstation antivirus clients to automatically scan all removable media the moment it's engaged.

Sure, it's an inconvenience for an end user, but it's an ironclad security policy in place at every secure military installation. Don't be fooled into thinking you're not part of the virus war as well.

7) - Apply all OS and application patches ASAP, preferably automatically.

Failure to secure your operating systems and application software with the latest patches is just asking for trouble. Every virus out there is designed to exploit a known vulnerability.

If you leave those vulnerabilities unpatched, you will eventually pay the price. Put a system in place that scans all your workstations and servers for missing patches and automatically initiates patch remediation without administrator involvement. Otherwise, your manual process will eventually fail and your network will pay the price.

8) - Always upgrade to the latest version of your antivirus software.

Software vendors issue upgraded versions for a reason (and it's not to milk your budget). They are providing a new and improved version with an enhanced feature set.

When you start relying on outdated tools to keep your network secure, you greatly increase the risk of a security breach. Weigh the cost of the upgrade against the cost of the downtime and lock your network down.

9) - Centrally configure all client workstations to the highest security settings.

Failing to use centralized configuration files and identical group policies on software settings makes support a nightmare. It also greatly increases your risk of a virus outbreak.

Review your standard configurations and make sure your workstations (and servers) are configured for maximum security. A good recent example is the DCOM/RPC service in Windows. It's not needed by any stretch of the imagination, but it's left enabled by most configurations. Very bad idea.

10) - Regularly scan your client workstations for viruses, trojans, spyware, and other malware on a weekly basis.

Don't rely exclusively on perimeter defenses and reactive processes. Initiate a clean sweep on at least a weekly schedule.

A virus or trojan can lay hidden or dormant on a workstation until activated by a line of code or by remote access (and then it's too late). For Windows clients, Pest Patrol does a good job of rooting out hidden agents capable of doing harm.

11) - Communicate security policies and virus alerts regularly with all users.

Don't keep your users in the dark and expect them to know what to do. Put out periodic reminders about not opening suspicious attachments or downloading files from the Internet.

Include a few statistics about the number of viruses caught weekly and monthly. Remind them to follow security policies. They are there for a reason.

12) - Have an Acceptable Internet/Email Usage Policy signed by every user that clearly defines Unacceptable Usage.

Every user should read and sign a copy of your company's Acceptable Usage Policy that covers Internet and Email Usage. They should also be given a photocopy of the signed Usage Policy for their records.

Make sure yours includes a clear definition of what is Unacceptable Usage. In case of a violation, review the Usage Policy with the end user and issue a written reprimand for their personnel file.

13) - Have a written escalation policy in place so your IT staff knows how to block the spread of a virus.

Your Business Continuity/Disaster Recovery planning should encompass a severe virus attack. Document all steps needed to isolate the virus and keep it from spreading.

Isolate the infection by taking immediate action to keep it from spreading. Don't forget you can actually pull the network plug on a few servers to keep things under control. It also won't hurt to run through a few simulations with your team to test their readiness.

14) - Have current system configuration documentation on all mail servers, application servers, workstations, etc. in case you need to restore.

Again, Business Continuity/Disaster Recovery plans should always include all necessary documentation of servers, workstations, routers, etc. Keep your records in at least two different places.

Outdated configuration information will hinder a quick recovery. Make sure you implement an on-demand tool that will automatically generate these configuration files and then do so, on a periodic basis.

15) - Have data recovery tools and processes in place.

Don't leave your team scrambling to assemble the tools and figure out the correct steps to take. Have all your tools on hand and your processes outlined before disaster strikes.

Otherwise, your recovery from a virus outbreak will take longer and cost a whole lot more.

16) - Keep full records of all virus attacks and remediation processes.

Document all virus remediation efforts for two reasons. First, to provide a record of what steps were taken. Second, to allow for a reversal of one or more steps, in case they were deficient or incorrect.

Recording the work performed can also be used as a business case for additional preventative resources.

Of course, all of these antivirus best practices will not completely protect your network if you don't follow best practices in other network security areas, but they will provide a high-level of protection all by themselves.

Make sure your network is secure by running vulnerability management systems that scan your network for security breaches 24x7.

After all, it’s your business. Let's be safe out there.

Greg Reynolds is a 22-year computer industry veteran and the President of **Net Sense**, an IT consulting firm based in Research Triangle Park, NC. **http://netsense.info**


$500 Gift Certificate $500
Presented to:_____
This certificate entitles the bearer to $500 off
any consulting engagement with Net Sense (Limit 1)