

## "Holistic" Enterprise Anti-Virus Protection

*Paul Schmehl* 2002-01-21

### "Holistic" Enterprise Anti-Virus Protection

by *Paul Schmehl*

last updated January 21, 2002

---

The year 2001 was the year of the enterprise virus attack. Code Red and Code Red II, Nimda, SirCam, Badtrans and Magistr all spread widely and all affected enterprises adversely. E-mail servers were stressed and in some cases shut down under the load of viral messages.

Vulnerable web servers were compromised and were taken offline to be rebuilt from backups. Sensitive corporate documents were e-mailed around the world. Trojan horses were planted on corporate computers and passwords and keystrokes of corporate users were e-mailed off to various accounts where the data could be sorted and used later for further compromise. After this onslaught, IT professionals worldwide took a deep breath over the holidays and wondered what would happen in 2002.

If it wasn't apparent at the beginning of 2001, it was certainly clear by the end of the year: enterprises worldwide must take a holistic approach to virus protection if they are going to get the threats under control. Rolling out desktop protection and expecting the end users to keep it up to date is obviously not going to work. (It never really did, but many seemed to believe that that was all they needed to do until 2001 came along and proved them wrong.)

This article will explore some strategies that can be used to help keep your enterprise relatively virus-free. The list is by no means exhaustive or definitive. Every IT group must decide what strategies best fit their organization's mission and provide the level of security they need without unnecessarily restricting the core activities of the business.

#### **Develop Sound Policies**

Any discussion of protective strategies would be incomplete without first mentioning policies. Sound, well-constructed policies are the bedrock of any successful security approach and should be considered very early in the process and implemented consistently throughout an organization. If no one has taken the time to decide what the appropriate policies to defend against virus infections are, then any implementation of technologies to deal with the problem will be less successful than it otherwise could be.

Sound policies should address the following; requirements for anti-virus protection including any proactive measures the organization will take to protect itself, appropriate responses to viral incidents and the consequences for violation of the policies. Many of the details must be left to the individual organization, for each company's requirements will necessarily be tailored to their IT environment and the needs of their business. However, some general concepts can provide a framework upon which to build a solid policy structure.

Up to date desktop protection should be required for every Windows computer that is connected to the corporate network. There should be no exceptions to this policy, for any reason. It should be a violation of the policy to disable or remove that protection under any circumstances. Many organizations may need to address the issue of remote Windows users as well. They may well want to require that every remote user have up to date protection in order to connect to the network. Other operating systems such as Macintosh and the various Unix platforms should also be addressed. Although they are not yet as prone to virus attack, each of them has had dangerous viruses written for them. Finally, policies for required virus protection for guest users, such as vendors and consultants, should be carefully considered as well.

In addition, consideration must be given to policies that address software patching. Every software program has weaknesses that are routinely discovered and exploited. A sound anti-virus policy must address how and when patching will be done and what the consequences will be when a failure occurs. In the case of serious incidents, such as Code Red, Nimda or the Adore worm, it may be appropriate to take the computer off line until its "owner" has repaired the breach and restored the system to sound operating condition, including installing the patches that might have prevented the problem to begin with. Repeated infections should result in an escalation of the disciplinary process up to and including termination in extreme cases.

Any proactive measures that affect corporate users should be clearly explained as well, including both the reasons for the measures and the consequences for attempting to bypass the protections. Some companies, reacting to the threat of webmail, have taken to blocking all the popular webmail sites such as Hotmail, Yahoo, Excite, etc. While at first glance this may appear attractive, the end result is unhappy users who will switch to webmail providers who are not yet on the blocking list. If any blocking measures are to be implemented, they should be part of a sound overall policy, they should be carefully planned and they should be clearly explained to the end user. Whenever possible, viable alternatives should be spelled out in the policy so there can be no arguments later that "this was the only way I could get it done".

## Protect The Desktop

In the final analysis, if the servers, workstations and desktop computers in your company are not protected against viruses, your corporation is exposed to serious risk. No amount of gateway protection, however well planned, can guarantee to keep viruses away from the desktop. There are so many infection vectors bringing viruses in to the enterprise that it simply isn't feasible to stop them all at the gateway. In addition to the tried and true floppy disk, viruses can arrive in any removable media, from zip disks to CD ROMs, to DVDs, to removable hard disks. Viruses can travel through e-mail; through web traffic; through instant messenger services, Internet Chat (IRC), FTP, handheld devices, cell phones, and file sharing programs like Morpheus, Napster and KaZaA; through any imaginable means that files can be transferred to a computer, some of which haven't even been invented yet.

Therefore desktop protection is absolutely crucial to any successful protection strategy. It is vital to have an enterprise license for anti-virus software and to find ways to automate its installation and updating. The desktop is too important to leave to chance. Any time an unprotected machine attaches to your network, it should be possible to detect its connection and force either the installation or update of anti-virus software or force the computer to disconnect. "Unprotected" should be defined as "not up to date", not "missing anti-virus software". Today viruses sometimes spread worldwide in twelve hours or less. Just having anti-virus software installed isn't good enough. You have to be able to update every computer in the enterprise within minutes of the release of an updated definition file. However, updating from the vendor's site during an outbreak can be problematic and in some cases impossible due to heavy traffic loads. Therefore enterprises should give serious consideration to creating a local site for updating. The anti-virus administrators can download once from the vendor site, and the entire network can be updated locally, without any of the problems associated with update distribution during a virus outbreak.

In addition to virus protection, methods must be found to keep servers, desktops and workstations properly patched. If the viruses of 2001 taught us anything, it is that keeping computers up to date on software patches will avoid many problems. Many viruses are written to take advantage of weaknesses in the OS or application software (such as e-mail clients or web browsers). Frequently, vendors have released patches months in advance of the first viral exploitation of a weakness. Yet the viruses are still successful because the number of unpatched machines is significant. If enterprises are going to get control of viruses, patching will have to become routine.

## **Educate The User**

Along with solid desktop protection, the basis of any sound anti-virus strategy is user education. Many IT professionals scoff at the idea, insisting that users are "too stupid" or "don't care". Nothing could be further from the truth. The "problem" with users is that they are not computer professionals. Their focus lies elsewhere. They have a job to do, and their computer is just one of the tools they use to get their job done. When an IT professional starts droning on about protocols and gateways and updates, most users become bored quickly because they don't understand the terminology. It's the job of a good IT department to communicate computer issues to their customers in terms the customer can understand.

It is not important that the end-user know the details of a virus. They only need to know what they need to do to protect themselves. Automating virus installations and updates as well as software patches eliminates a great deal of end-user confusion. (Am I up to date? What do I need to do to stay up to date? How do I update? Etc., etc.) Instructions to end-users should be given in general terms; what to do when a strange attachment arrives, how to recognize potentially "bad" programs, what actions to avoid when connected to the network, how to work cooperatively with the protections that are in place.

## **Fortify The Gateway**

Once you have virus protection at the desktop in place, you need to analyze your network assets carefully to determine how best to build protection at the gateway. E-mail is very important because it's the present method of choice for distributing viruses. However, other methods of distribution may predominate in the future. Just as the floppy disk gave way to the e-mail client, the e-mail client may give way to the web browser or the instant messenger or the cell phone.

When you think about how traffic flows in and out of a network, some obvious "choke points" appear. One area is the Internet connection itself. A network intrusion detection device may be put to good use in this area, as may a firewall. Many modern firewalls and IDS systems have the ability to detect certain types of virus attacks such as Code Red and Nimda, alert network support personnel and immediately drop the connection. Some "intelligent" routing and switching equipment comes with the ability to foil certain types of attacks. Cisco's "NBAR" (network based application recognition) is an example of this.

In some cases, based on business goals, it may be possible to block certain ports, preventing some types of attacks from being successful. This can be particularly helpful with viruses like Badtrans that plant trojans on computers and send passwords and even keystrokes to an attacker's web site. The range of trojans that are easily available on the Internet is so great that some businesses may want to consider adopting a policy of "white listing" ports. Rather than trying to keep up with the list of ports that are known to be used by malicious programs, white listing takes the approach of closing all ports at the gateway and only opening ports that are known to be needed by the business. Cognizant of this approach, virus writers have begun concentrating their attacks on ports which cannot be closed, such as HTTP, e-mail, FTP, etc.

### **Protect Critical Services**

Once the gateway has been protected, focus on critical services. Since the bulk of viruses attack through e-mail and the web right now, those two services should get special attention. There are a large number of products available today that provide content filtering. It's even possible to create "home-grown" solutions by using the existing capabilities of the daemons that provide service. More and more e-mail servers have content filtering capabilities built in. It's possible to block e-mail, for example, that has an attachment with an extension that is on the "forbidden" list. This technique is essentially the first line of defense for Messagelabs, the popular e-mail-filtering provider.

There are also products that are designed to scan for viruses in e-mail, web and ftp traffic. Although they suffer from the same weakness that all anti-virus software has, the need to be constantly updated, they can provide an effective adjunct to the other measures already discussed.

In summary, to fight the virus battle, enterprises must take a holistic approach to virus protection. Every aspect of the enterprise should be examined for ways to lessen the impact of viruses so that the organization can fight off viruses in a coordinated fashion. Once effective measures are in place, the IT staff should keep a vigilant watch for new attack methodologies and devise strategies to deal with them. By doing this, the enterprise can remain relatively virus-free, and the end-users, the customers of IT, can concentrate on the success of the business.

*Paul Schmehl is a Technical Support Services Manager with over 25 years experience. He is currently employed in IT management in higher education, in enterprise-wide technical support, help desk management*

*and anti-virus protection. Involved in many new technology projects, web site development and security-related issues. Paul is also a founding member of [AVIEN](#).*

[Privacy Statement](#)

Copyright 2006, SecurityFocus