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.

Security Management View of Implementing Enterprise Antivirus Protection

This paper provides practical information to consider when planning the deployment, upgrade, design, or engineering of an enterprise antivirus solution. Antivirus solutions usually focus on Microsoft Windows environments, but this paper adds some tangential notes about Macintosh and UNIX variants. Included are descriptions of security management activities that increase the benefit of antivirus product(s) deployment in an enterprise setting, such as describing deployment design within a "layers of defense" paradigm. Ot...

Copyright SANS Institute

Author Retains Full Rights

AD

Streamline IT security environments and compliance processes.

Transforming IT Management.

Title: Security Management View of Implementing Enterprise Antivirus Protection

Practical: GIAC Security Essentials Certification 1.4b, Option 1

By: Mike Stowe

Course Location: Online

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Table of Contents 2
1 Abstract 3
2 Introduction 3
2.1 Caveats 3
3 Security Management in Layers of Defense 4
3.1 Layer 1 – Security Gateway with Public Internet 6
3.2 Layer 2 – Scanning Content 8
3.3 Layer 3 –Email Servers 10
3.3.1 Separate Outbound Email Paths 10
3.4 Layer 1, 2, 3 – Combining 11
3.5 Layer 4 – File Servers 12
3.6 Layer 5 – Workstations, Desktops, Laptops, or PDA 13
3.7 Layer 6 – User Community 15
4 Security Management Processes with Antivirus Technologies 16
4.1Product Management 16
4.1.1 Testing New Signatures 16
4.1.2 Distributing Signatures 16
4.1.3 Deploying Antivirus Agents 17
4.2 Monitoring 17
4.3 Prevention 18
4.4 Intrusion Detection 18
4.5 Incident Response 18
4.5 1Preparation 19
4.5 2 Identification 19
4.5 3 Containment 19
4.5 4 Eradication 19
4.5.5 Recovery 19
4.5.6 Lessons Learned 19
4.6 Management Reporting 20
5 Conclusion 20
7 References 22

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1 Abstract

This paper provides practical information to consider when planning the deployment, upgrade, design, or engineering of an enterprise antivirus solution. Antivirus solutions usually focus on Microsoft Windows environments, but this paper adds some tangential notes about Macintosh and UNIX variants.

Included are descriptions of security management activities that increase the benefit of antivirus product(s) deployment in an enterprise setting, such as describing deployment design within a "layers of defense" paradigm. Other facets of operating, administering, and maintaining antivirus technologies are also described in addition to the identification of some management metrics that quantify the value of antivirus deployment.

2 Introduction

Studying antivirus solutions has been ongoing for some time. (Attis, ISSA) Stephen Cobb notes that organizations can increase the benefits of antivirus products and technologies by considering the security management view of antivirus deployment. This includes:

- The security context of implementing antivirus solutions into a network-computing configuration
- The security configuration options of antivirus technologies
- The tools or processes related to operating, administering, maintaining or providing control metrics about an antivirus deployment

"If you do the right things with AV software, you're well protected," Cobb explains. "But an awful lot of people don't configure or install it properly, nor do they update. We need things that can protect and defend systems automatically. That isn't being done at the moment." (Saita)

2.1 Caveats

This paper's reference to antivirus technology is a generic reference to selected types of malware. In this paper, antivirus technology refers to the software products or tools that claim to detect, block, repair, disable, erase, or quarantine nefarious software known as a computer virus. (New Hacker's Dictionary) Most of these products and tools also claim to address worms and Trojan horses.

The paper is structured to add relevant references in selected locations about spam plus malicious code being activated by surfing the web and engaging active local content such as java applets or ActiveX controls. (Zager)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The information in this paper should apply to large to small organizations as long as an organization uses an enterprise deployment solution. Here, "enterprise deployment" refers to uniform distribution, operation, administration, and maintenance across all departments of a given organization. And the information in this paper should apply in a bureaucratic corporate setting, dot.com startups, or university environments.

3 Security Management in Layers of Defense

One important aspect of security management is to consider the relative placement and interaction of antivirus products, adjunct tools, and processes within the context of a defense-in depth-strategy. (VanMeter, Northcutt Chapter 22) This paper applies the defense-in-depth concept by identifying layers of defense follows:

Layer 1 – Internet visible platforms
Layer 2 – content scanning servers
Layer 3 – email servers
Layer 4 - file servers
Layer 5 – desktop, laptop, workstations, PDA
Layer 6 – User community

Figure 1 illustrates these layers for email messages. Figure 2 illustrates these layers for files and malicious code. Each layer is described in a separate section below.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

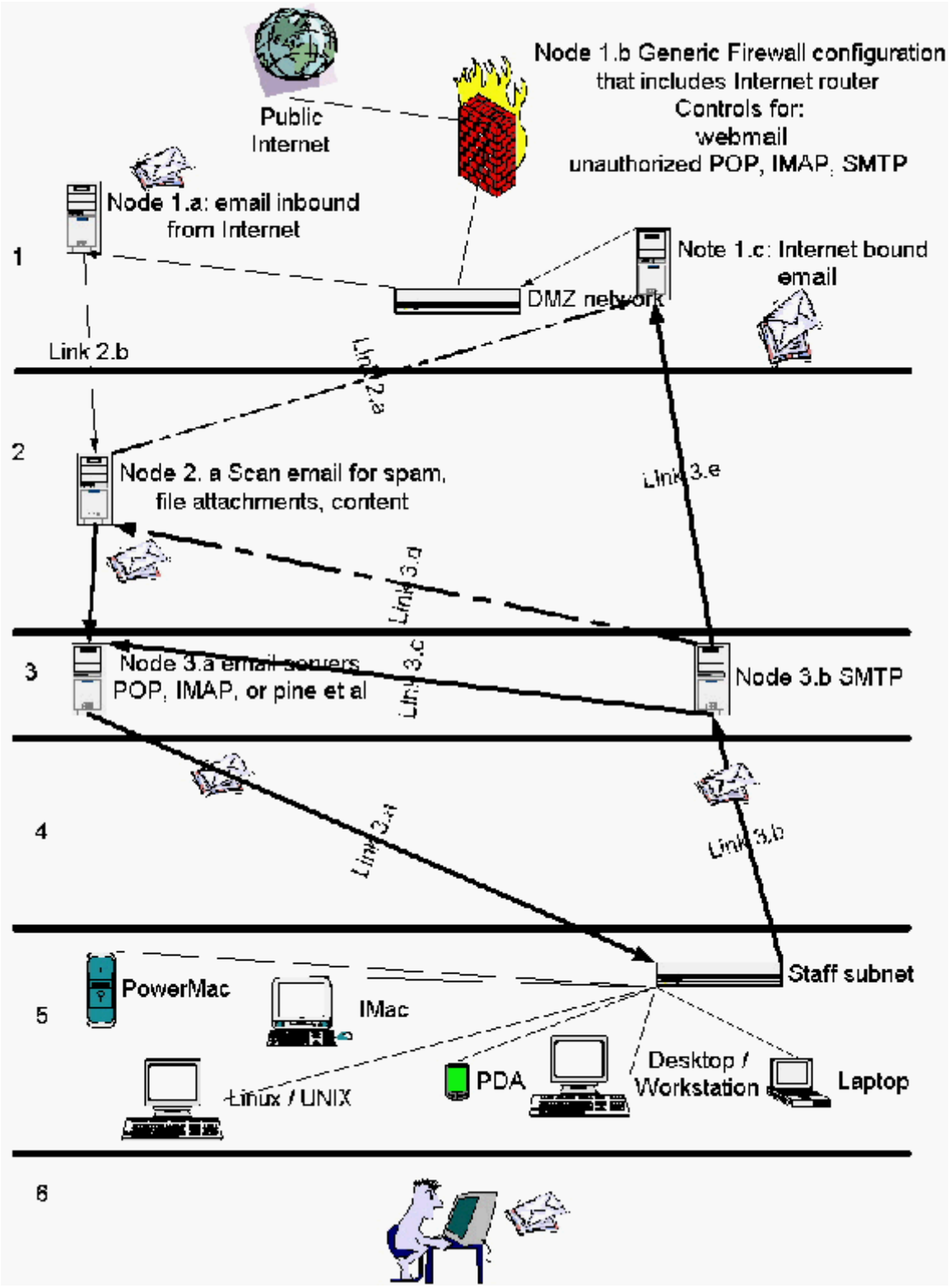

Figure 1 – Antivirus Deployment in Layers of Defense – Email Messages

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3.1 Layer 1 – Security Gateway with Public Internet

Layer 1 and Layer 2 cover the kinds of protection that are often considered as part of a firewall and DMZ configuration. Usually a firewall and an email server are visible from the public Internet.

As shown in Figure 1, Node 1.a , there is usually an email server that receives the incoming traffic destined for an organization based on DNS MX settings, or transfers the email traffic from the upstream ISP email servers. When managing the security of these Internet-visible, inbound email platforms, there are advantages of using a platform dedicated to the inbound email function with a secure operating system, such as OpenBSD, and an email tool, such as postfix, developed to counter sendmail exploits. (Postfix) Layer 1 inbound email servers are a logical location to refuse email based on:

- The various blacklist services that can be enabled, usually in sendmail or postfix configuration files (Mail-Abuse)
- Email servers that you know to be repeat virus and spam sources, or as sources of SMTP probes from your Intrusion Detection System

Depending on the rigor needed to control virus infections, there might also be a need to restrict the user community from accepting mail attachments that could be accessed outside the anitvirus deployment design. Figure 1, Node 1.b can be configured to deny POP and IMAP access to external email servers. Some organizations might have to go so far as to restrict access to web mail services with firewall controls. Experience shows that blocking all web mail servers is an arduous experience. Even blocking the web mail servers of the major providers like AOL, Hotmail, and Yahoo by DNS name involves periodic maintenance.

If there is a need to control the administrative overhead associated with propagating virus infections outside an organization, you can configure a firewall's access control filters to deny the use of non-organization SMTP servers from user email clients. Depending on the structure of an organization's Intranet, similar IMAP, POP and SMTP access controls can also be placed at the border router(s) associated with Layer 5, as shown in Figure 1.

Hopefully, sharing Windows folders over the Internet is not a requirement and the firewall shown in Figure 2, Node 1.b can be configured to filter SMB packets. If an organization has excess security administration resources and has the platforms that can absorb the overhead of extensive filters, you can also add peer-to-peer file sharing and instant messaging to the firewall controls. (Practicallynetworked)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

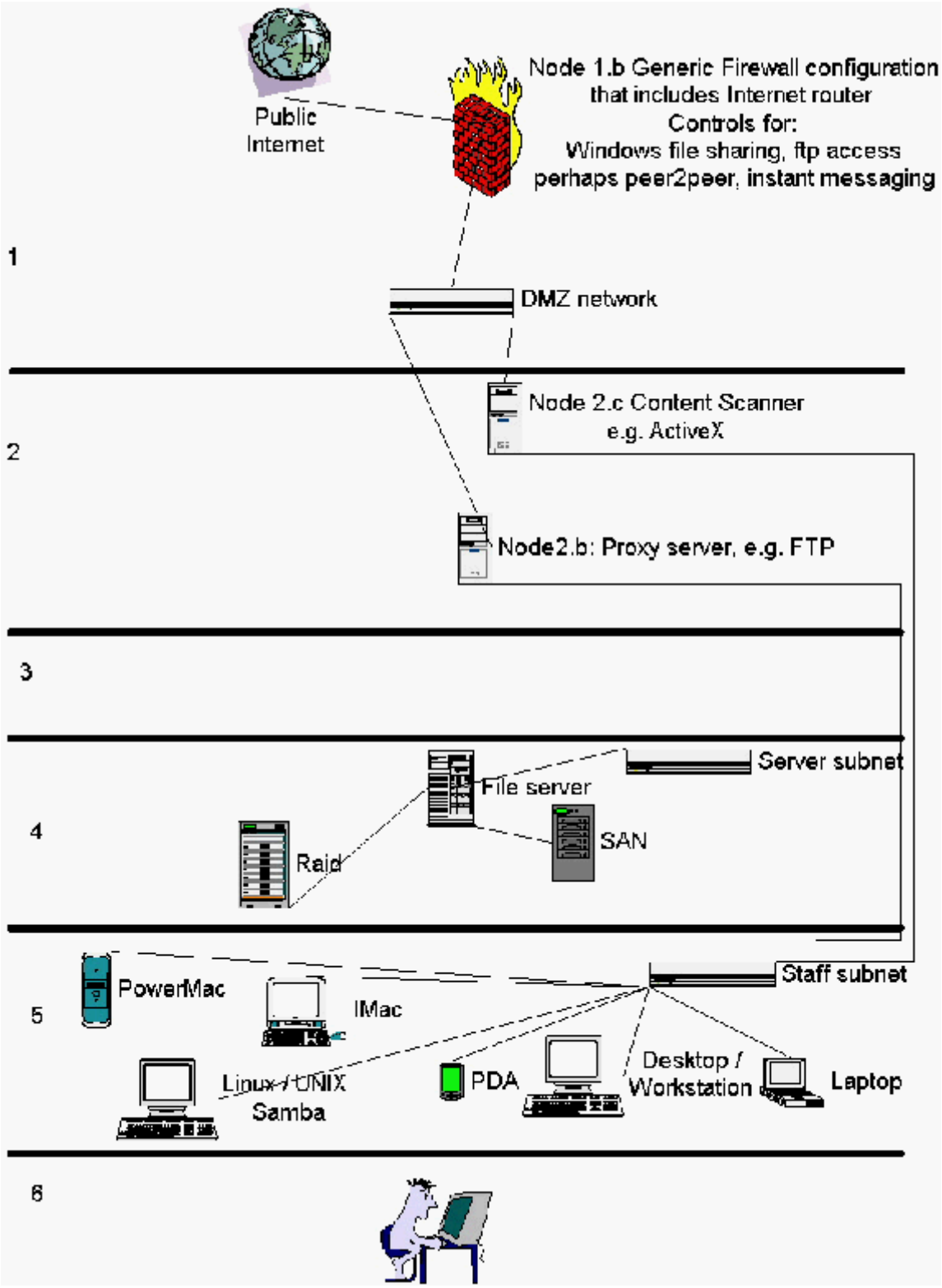

Figure 2 – Antivirus Deployment in Layers of Defense – Files and Malicious Code

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The firewall logs in Layer 1 also have a role in antivirus deployment. These logs can be parsed for attempts to originate traffic with well-known virus ports. (von Braun, Banes) This security management control process should be customized carefully based on past experience and current activity since backdoor agents have used so many ports. (SANS)

The context for the outbound mail server, Node 1.c in Figure 1, is explained in a later section on Layer 3's email servers.

The anitvirus security controls placed in Layer 1 function primarily as

- Spigots to turn off access to the Internet, if necessary, to contain a virus infection
- Filters that lower the overhead of processing messages and files in lower layers
- Controls that constrain the user community to using an organization's antivirus design

3.2 Layer 2 – Scanning Content

The Layer 2 antivirus functions typically focus on scanning the content of messages and files, primarily those exchanged with the public Internet. Layer 2 also addresses malware in the form of active local content.

Figure 1, Node 2.a shares in Layer 2 functionality by

- Processing email attachments
- Scanning email text for questionable content, usually for spam scoring but perhaps as part of a security investigation
- Identifying spam based on the email content
- Providing blacklist or denial service, if those were not included in Layer1

Figure 2, Node 2.b scans inbound traffic for infected files. Usually this in the form of specialized proxy server capable of scanning specific kinds traffic, such as ftp transfers. (NAI)

Figure 2, Node 2.c scans inbound traffic for malicious code. This can take the form of a service integrated with the firewall. (Check Point Software) Quite often this focuses on specific technologies, such as ActiveX control attacks or malicious Java applets. (Finjan)

You can scan outbound traffic from an organization's web and ftp servers or user file transmissions. But this is a subject worthy of different paper. It requires some DMZ, ftp, and web server configurations not shown in Figure 2.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

There are a variety of antivirus solutions for Node 2.a that work with different email technologies at Layer 1 and Layer 3. (Clearswift) Sometimes they combine antivirus and anti-spam protection in one antivirus product. (Tumbleweed) Usually, the products or tools that fit best fulfill an SMTP relay role.

Sometimes a variant of a freeware tool called 'Sanitizer' is used on Node 2.a. (ANOMY) Sanitizer variants take a different approach than some commercial tools because it does not deliver attachments with specified file suffixes. Or, it delivers files with specified suffixes changed to a harmless suffix (also known as 'defang') that requires manual effort by a user to open the file.

In some cases, design criteria dictate that a single solution be implemented for Figure 1, Node 1.a and Node 2.a. The major tradeoffs in these situations are

- Simplicity in the number of functional relationships and product administration
- Risk of the compromising Node 2.a functionality on a platform visible to the Internet

There are also products that consolidate Nodes 2.a, 2.b, and 2.c in a variety of ways. (NAI, Trend Micro)

One security management decision for Layer 2 is about Figure 1 Node 2.a notifying the sender or recipient of an infected email attachment. Some considerations are

- The implications of sending such notifications to spoofed origination addresses
- That an external party might be using such information to map the capabilities of an antivirus deployment.

Notifications the Intranet community should specify the user's expected course of action, such as isolating the file reported as an infected

There are also hardware-based solutions that might allow a single solution to cover the function of Nodes 2.a, 2.b and 2.c. (Fortinet)

The anitvirus security controls placed in Layer 2 function primarily as

- Large scale filters for inbound email, files and malicious code.
- Lower the chance that an infected message will reach a layer 5 platform and potentially bypass a Layer 5 antivirus technology, especially where Outlook clients are allowed to use message preview options:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3.3 Layer 3 –Email Servers

In smaller organizations, the usual scenario is just one email server providing the functionality shown in Figure 2 for Node 3.a. In larger or distributed organizations, there are multiple POP or IMAP servers. In some organizations, Node 3.a comprises multiple products, such as sendmail, postfix, Exchange, or Lotus Notes.

If Exchange is used on a Layer 3 email server, you should run an antivirus solution on each Exchange server or on each email client, or on both. (Chau) Any single Exchange server can be turned into a virus propagation engine, as many serious virus writers target Exchange and Outlook, the preferred email client for Exchange users. If an antivirus solution is placed on the Exchange server, most organizations have the Exchange server(s) combining the functions shown in Figure 2 for Node 2.a and 3.a.

If Node 3.a is a UNIX server(s), then managing the security of the configuration includes choosing the mail product. If no special sendmail requirements are necessary, postfix is a good choice. (Postfix) Other email server solutions, such has Lotus Notes, have antivirus solutions as well. (Trend Micro, About)

Sometimes there is a remote access capability to Layer 3 email servers, either through VPN connections, direct dial-up access, or direct Internet access. Some VPN gateways can be configured to verify the existence of selected antivirus solutions on the remote computer. These gateways enable dial, DSL, and cable modem access. (Demaria) But if the stability, support, and bandwidth limitations of a VPN gateway do not suffice for an organization, then direct access to Node 3.a still poses a risk for injecting infected email into an organization. Grappling with the support, privacy, and operational issues of solving this problem requires research and further work.

While it is beyond the scope of this paper, remember that POP and IMAP access should require authentication.

The anitvirus security controls placed in Layer 3function primarily as

- Spigots to turn off access to the email messages from Layer 5
- Filters for email exchanged within the Intranet

3.3.1 Separate Outbound Email Paths

It is not necessary to use the same path for inbound and outbound mail. A separate or partially separate outbound mail path can also be a useful security management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A separate SMTP outbound path similar to Node 3.b, that functions as an SMTP relay to either Node 2.a or 1.c removes dependency on the inbound email servers. It also provides the option to control outbound email message traffic without affecting inbound traffic. This is a definite advantage if an organization needs to control Microsoft Exchange without Exchange-specific antivirus solutions installed or control Exchange with non-Outlook clients or. If an organization runs Exchange without an antivirus solution installed, it should seriously consider directing outbound email traffic through Node 3.b. This traffic path is not shown on Figure 1.

By controlling the configuration of link 3.c, 3.d and 3.e, Node 3.b can queue or redirect outbound traffic without impacting users. The normal flow of traffic is over links 3.c and 3.e, depending on the Internet or Intranet email destination. These links can be shut down when Node 3.a or Node 1.c undergoes maintenance.

If the frequency of outbound email infections is low, then it is beneficial to keep the inbound and outbound email paths separate except during a virus outbreak. The At the time of a virus outbreak, an organization can help control the spread of a virus by having all outbound mail directed to Figure 2 Node 2.a via link 3.d by changing the configuration file on Node 3.b. This change effectively shuts down links 3.c and 3.e.

Using a configuration change with Node 3.b is superior to adjusting the SMTP parameters of email clients or to changing DNS addresses of SMTP servers because of the speed and effectiveness of the change. Geographically distributed organizations recognize that Node 3.b could be instantiated in multiple locations. Node 2.a needs to be changed during this process so it can direct Internet-bound email to Node 1.c over link 2.a.

Controlling outbound email traffic through Node 3.b can help, as follows:

- Lower the risk that outbound email traffic will overload Node 2.a
- Provide a means to queue traffic while Nodes 3.a, 2.a or 1.c are upgraded, virus signatures are tested, or while one waits for updated virus signatures to address the outbreak of a new virus

One potential obstacle of a separate email path is if you want to use authenticated SMTP and cannot integrate the authentication technologies of Node 3.a and Node 3.b. In addition, some bundled client and server solutions require Node 3.a to be 'the' SMTP server.

3.4 Layer 1, 2, 3 – Combining

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sometimes an organization has to combine some of these layers of defense based on the resources available. Choosing the technologies and the underlying platforms often involves the art of balancing business, economic, or engineering tradeoffs regarding the following:

- Cost
- Time to deploy and operate
- Function provided
- Ease of operation
- Risk in using more platforms (and maybe more complex network connections) dedicated to antivirus functions and only essential network computing services
- Risk in using fewer platforms but more complex antivirus configurations; possibly mixed with services that do not relate to a antivirus solution

There are some products that provide 'integrated solutions' on a single platform allowing one to combine layers, usually the email aspect of Layers 1, Layer 2, and sometimes Layer 3. (Central Command, Mailservers) In these cases, products that function as SMTP relays are usually excluded if Layer 3 in combined with Layer 2.

The paradigm used with double-blind firewalls that utilize different operating systems and firewall solutions can also apply to anitvirus deployment. If resources permit, using different antivirus products in Layers 2, 3, 4, or 5 can strengthen the viability of the enterprise antivirus deployment. (Northcutt, Page 260)

3.5 Layer 4 – File Servers

The installation of antivirus software on file servers should be configured to minimize the distribution of infected files to the user community. Given the ever-increasing size of file server storage, one concern is starting virus scans that might not complete in the allotted time schedule. As such, the configuration of the drives and directories to be scanned at Layer 4 (and Layer 5) should consider

- Configuring directories or drives to isolate (and ignore) file types that are incapable of infection
- Using products that, in addition to having the capability for automatic scheduling and scanning the local platform, provide multiple schedules so scans of file types that pose a much lower risk to particular organization, such as PDF files perhaps, can be scanned less frequently. (F-Secure)
- Coordinating the scanning schedule with the backup schedule

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Validating that the backup configuration and system recovery process can recover 'good' versions of infected files or rebuild a platform ravaged by a virus
- Excluding folders where virus-infected files that cannot be repaired are stored
- Excluding network drives from scanning
- Using the ability of an antivirus solution to distinguish complex drive configurations, such as mirrored disks
- Automatically enforcing antivirus product parameters
- Automatically distributing and installing virus signatures on a periodic schedule (once a week seems to work for the current situation) or on-demand for containing new viruses

Two special exceptions to not scanning network drives need to be noted.

1. Remotely scanning Samba folders as network drives where no local scan is possible is useful since the host is usually a variant of UNIX (Pardo)
2. Scanning network-attached storage and storage-area networks should only be scanned once per designated time period, regardless of the network or host channel attachments (Trend Micro)

Finally, if an organization's security policy allows, disable host scripting on Windows platforms. This also can apply at Layer 5. Use a systems management tool, such as SMS, or simply use the AT command, to periodically execute the noscript tool through the command line using only the silent option. (Symantec, Scripting Host)

3.6 Layer 5 – Workstations, Desktops, Laptops, or PDA

Quite often the main focus of an antivirus effort is limited to Layer 4 and Layer 5. This might result from resource constraints, vendor hype, or a lack of awareness of the advantages for of a defense in depth approach.

The Layer 4 – File Servers section earlier noted several configuration issues that apply to Layer 5 too. Remember that it is not a given that Layer 1 through 4 defenses will detect all infected attachments or files, especially given the rate of virus creation and evasion. (Security NNOV, Northcutt, page 260) Even if an organization uses alternatives to Outlook and Explorer, it is still possible that floppy disks, CDs, and ftp file transfers will introduce viruses. Depending on what your security policy allows and the filtering capacity of your firewall, instant message tools, peer-to-peer file sharing, and the use of web mail are probable sources of virus infection at Layer 5.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If you use multiple virus detection technologies on a single platform, it is usually necessary to exclude the 'virus found in this file' folder of one technology from the scanning configuration of the other product(s). This situation usually occurs during the transition of one antivirus product to another, adding a chosen antivirus solution onto a turnkey desktop or laptop configuration. This is also true with the use of personal firewalls that have an option for scanning email attachments, such as Zonealarm.

If an organization uses Microsoft Outlook for email in either Windows or Macintosh environments, and your users can accommodate the inconvenience, you should consider turning off the message preview options. (Banes)

Another item to configure is specifying the time of automated scans. Typically it is important that the user community understand they should not turn off their workstation or laptop. Besides coordination with backup processes, the behavior of the user community needs to be considered. You might have good luck specifying layer 5 scans for 2 am and asking laptop users to plug in their machines and turn them on while at home or on the road. Workstations being used 24x7 can be a logistical challenge. In such cases, the automated scan might be scheduled during a lunch break.

Some final items to think about with Layer 5 are:

- Specifying the SMTP server for email clients. See the section on Layer 3 – Email, for more information-
- Installing Notes or Microsoft Exchange plug-ins for certain email clients (Symantec Enterprise Solutions, Trend Micro)
- Integrating some antivirus products with instant messaging tools (Symantec Instant Messaging)
- Deleting enterprise software usually involves some form of administrative access because the antivirus configuration is 'locked' and some products even require an additional password, which should be specified so users don't uninstall antivirus technologies; and which needs to be changed if it disclosed (Symantec Enterprise Solutions)
- Although they are rarely part of an enterprise antivirus solution, the following Layer 5 platforms do have antivirus solutions. Using these solutions can help prevent infections from affecting an enterprise configuration. However, they rarely integrate with enterprise solutions concerning automated distribution of agents, virus signatures, or centralized detection reporting

    - PDA (Symantec Palm)
    - UNIX variants, such as Linux, BSD (Central Command Linux)
    - Netware (ICSA)
    - Macintosh OS8/9 and OSX (ICSA)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3.7 Layer 6 – User Community

The user community is the linchpin in any antivirus deployment. Never underestimate the value of educating users about using email clients, using common sense in the Internet experience, and noticing suspicious behavior.

While many security programs emphasizes that security is everyone's responsibility, organizations are well advised to be balance the burden placed on your user community in the overall antivirus effort. The less manual effort involved, the less security contributes to the general overhead of an organization. Some security management capabilities that you need to think about at Layer 6 are

- The advantage of installing virus signature updates without user intervention
- The advantage of automatically repairing viruses, if they are repairable
- The advantage of automatically setting aside infected files that cannot be repaired so that skilled practitioners can analyze them and users don't propagate the infected files
- The level of effort, and the errors introduced, by users renaming documents affected by the 'Sanitizer', noted in the Layer 2—Scanning Content section, to 'defang' attachments
- An effective and efficient method for users to notify the support staff that they suspect a virus infection

Security education and training often proves to be the most valuable security prevention investment in the antivirus arsenal. (Gullet) The best approach is to minimize user interaction with antivirus processes except to stress the importance with users about the following:

- Not opening email attachments unless the user is sure of the source and the attachment is expected
- Not downloading or copying files from unknown sources
- Using caution with technologies like instant messaging, peer-to-peer file share, Windows file sharing, ftp file transfers, and so on.
- Using antivirus solutions on home computers, especially if remote access to Node 3.a is possible
- Being careful about posting a valid email address in a newsgroup
- Being cautious about registering their email address at web sites
- Noting suspicious behavior like independent mouse movement or social engineering queries

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4 Security Management Processes with Antivirus Technologies

Other areas, besides just the placement and configuration of antivirus security technologies, need to be considered. (Banes) Deployment personnel need to plan, organize, and control the-

- Administration and maintenance of the antivirus technologies
- Operational context of the antivirus configuration
- Use of management data about the effectiveness or efficiency of the antivirus configuration

4.1Product Management

You need to manage the antivirus products. Typically, this involves distributing virus signatures or scanning engine updates. Given the increasing amount of virus activity, weekly updates seem appropriate at most locations. Before distribution, however, you should examine the new testing signature files or scanning engine updates. At Layer 4 and Layer 5, the antivirus software integrates closely with the operating system to intercept a variety of system events, such as moving a file.

4.1.1 Testing New Signatures

More than one vendor has distributed a new signature file or scanning engine update that has caused the dreaded 'blue screen' on Windows platforms. And one needs to consider the possibility that the Internet distribution site has been compromised. (Lubow) Limiting the damage from these situations can prevent significant loss of productivity and prevent damage to the reputation of the security department.

For Layer 4 and Layer 5, test the signature or scanning engine update on the same mix of platforms that the general antivirus client population is using. It is not a given that a problem affects all versions of Windows, Macintosh, and so on. After installing the update, perform a general scan on the test platform(s), then reboot them. Install a test eicar file (Eicar) and see if the test file is detected in real-time. Do another general scan if you generally do not trust Windows behavior.

Testing Layer 2 signature updates usually involved sending a message that has the eicar file attached or transmitting the eicar file through the inbound file exchange proxy.

4.1.2 Distributing Signatures

After testing the virus signatures, it works best if the virus signatures can be distributed internally. (Lynxwiler) This is usually much faster given Intranet bandwidth. This also prevents mass outages due to faulty signatures or scanning engine updates. Plus there will have less traffic through the firewall.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Some products have this 'internal distribution server' capability built in. (Symantec Enterprise Solutions, Trend Micro) Other system management tools, such as SMS, can distribute the relevant antivirus signatures to servers and desktops.

4.1.3 Deploying Antivirus Agents

Another part of the security management plan is how to deploy antivirus client software to the server and desktop platforms in Layer 4 and Layer 5. This deployment is usually limited to Windows platforms for automated solutions. (Bothelo) Sometimes system management tools, such as SMS, help facilitate this if the chosen antivirus product does not provide the function. In some cases, a custom login script for Windows platforms can work. For Macintosh platforms, it is often necessary to install the product upgrades manually.

4.2 Monitoring

The various components of the antivirus technologies need to be monitored. Monitoring reveals clues about refinements necessary in the overall antivirus design, adjustments necessary on particular tools, and the need for more control metrics.

Exception control process are needed to detect

- Errors in the distribution or installation of virus signature updates
- Failures in scheduled platform scans
- Excessive viruses detected but not repaired

Often, the antivirus tools installed automatically report virus detection. This is useful for the reports described in the management reporting section. Sometimes an organization needs to augment an antivirus product to get effective reporting. (Lynxwiler) Plus, some analysis of detection patterns is important. The simple patterns to begin with are-

- Method of entry-how did the virus gain access to the platform?
- Virus type, category and variant-or example, is there a sudden increase in Nimda detections?
- Platform detection --is there a pattern in the frequency, timing or order of platform infection?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.3 Prevention

Besides using just antivirus products to prevent or detect the entry of infected files into the Intranet, an organization might consider a daily security management task that checks the web sites of chosen vendors or one of the popular virus reporting web sites. (Virus Bulletin) Often, there is enough information provided that can be used to

- Update or customize intrusion detection signatures
- Provide port information that can be used in scanning intranet platforms on a proactive basis
- Formulate communiqués to the user community warning them of potential dangers at unscrupulous web sites or in email messages

4.4 Intrusion Detection

Some information from the prevention step can also assist with detection--sometimes communiqués to the system administration staff are warranted to help them recognize behaviors that indicate a successful virus infection.

If you have intrusion detection sensors on Link 2.b shown in Figure 1, you can improve productivity by disabling the spam, virus, Trojan, and worm signature rules on inbound traffic. Any alerts are obviated by the antivirus functions of platform Node 2.a.

Leaving those rules enabled for outbound traffic arriving at Node 1.c or Node 3.b can serve as a useful control mechanism that indicates when your antivirus technologies have inadvertently been disabled or incorrectly maintained.

Intrusion sensors on Link 3.a should have any applicable spam, virus, Trojan, and worm rules enabled to serve as the control indicator about the utility of your Node 3.a antivirus solution. Other sensors on the server network or staff network probably don't need the rules activated.

4.5 Incident Response

The security awareness education in Layer 6 should include how to register a potential virus infection through a web page or an organization's help desk. Sometime distributing stickers that contain this information helps users. They might attach these to their monitors or phones. But an organization somehow needs to monitor user perceptions that somehow a platform has a virus infection that the antivirus software solutions have missed.

If a virus detection is really an infection and the repair cannot be automatically completed, then a simple incident response procedure needs to be followed. A sample set of steps for incident handling follows.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.5 1Preparation

- Educating the user community in behaviors that might suggest their platform has been compromised by a virus (See the previous section describing Layer 6).
- Installing tools, such as Languard or Tripwire, that monitor the file integrity of key system or application files,.

4.5 2 Identification

The antivirus tools that detect the virus infection often identify it. Even if a specific virus is not identified, the tools usually identify the generic category of the infections, such as 'Backdoor', most likely without leading to a false positive situation. (Northcutt, page 259).

4.5 3 Containment

Decide about severing network connections of the infected platform(s), the various email links noted in Figure 2, and the connections to the Internet--plus any extranet connections.

4.5 4 Eradication

- Research the nature of the virus infection
- Decide whether to rebuild or repair the infected platform
    - Acquire virus repair tools. Some vendors provide such tools as freeware. (Symantec Tools, McAfee)
    - Repair the infected platform
      or
    - Rebuild the platform from system recovery and backup files

4.5.5 Recovery

Run a scan with the local antivirus tool to verify eradication
Run a vulnerability scan from an external source to verify the functional profile of the platform and identify a well-known virus ports
Run any relevant application regression tests

4.5.6 Lessons Learned

Repairing infected platforms is an expensive use of system administrator resources. These repairs also impact user productivity. Therefore, it is important to determine any refinements to the antivirus deployment plan that can avoid future infections.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.6 Management Reporting

Unless your company is part of the information security industry or your company considers information security a core competency, the most common communication with management antivirus solutions is about money, user impact, and using security staff resources.

Communicating the fixed and variable acquisition costs and ongoing maintenance are useful for the cash-flow part of a business case. It is also worthwhile thinking about other financial metrics that illustrate the effectiveness of the enterprise management solution. Combining costs noted in the business case and providing realistic estimates of ongoing operational costs can apprise management of cost metrics based on the historical cost of antivirus deployment.

One metric is the cost per seat per technical solution. For example, what is the historical cost of the antivirus solution used in Layer 4 and Layer 5 divided by the number of platforms. Or what is the historical cost divided by the number of detections and automatic repairs? Or what is the historical cost of antivirus technologies at Layer 2 and Layer 3 divided by the number of email users

Another metric is the cost per message per technical solution. For example, what are the separate historical costs for Nodes 2.a, 2.b, and 2.c divided by the number of messages they processed? Or what is the historical cost divided by the number of detections and automatic repairs?

Eventually, one might want to convert some of the historical data presented to management into rolling average costs that can show the trend in the return on investment in antivirus technologies.

Depending on how a management team tracks business case proposals, there might be an opportunity to occasionally reiterate the productivity gains made by enterprise antivirus deploy, such as time saved in:

- Rebuilding infected platforms
- Repairing infected platforms
- Automating virus signature updates both for the user community and containing a virus outbreak
- Problem diagnosis of aberrant platform behavior

5 Conclusion

You can use this paper as a template to describe what will, and will not be, part of the design and engineering of an organization's antivirus deployment. By considering the network-computing context of antivirus technologies, an organization can improve the benefits derived from enterprise antivirus deployment (Schemel). An organization is then more likely prepared to deal with more advanced antivirus deployment issues, including

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Encrypted email messages
- VPN tunnels that reach Layer 4 or Layer 5 platforms, hiding email and file transmissions
- The potential integration of antivirus and host based firewalls
- Encrypted files and file systems
- Outbound file transmission
- Java and ActiveX controls supplied by an organization's web servers
- Using products, such as Symantec's Carrierscan, in product development

The concepts discussed in this paper can be implemented in phases to conserve staff and financial resources.

By augmenting generic antivirus functionality (ICSA) with a 'layer of defense' approach an organization can

- Minimize the probability of virus infections
- Contain the spread of a virus infection, protecting staff productivity
- Minimize the system administration overhead of controlling virus propagation
- Understand what will happen for if a node in Figure 1 or Figure 2—which has deficient antivirus functionality, is inoperable or is compromised

Using important management features of the antivirus technologies reduces the involvement of the community by automatically updating virus signatures, enforcing local antivirus configuration parameters, and controlling the local scanning schedule. (Trend Micro, Symantec Enterprise Solutions)

Finally, it is important to periodically communicate with an organization's management hierarchy to sustain claims of improved productivity, operational improvements, and to show the value of the investment in an enterprise antivirus deployment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7 References

Attis, Ben. Internet History. California State University. June 5, 1997.
URL: http://lrc.csun.edu/~battias/454/sum97/hist.html (November 22, 2002)

ISSA (Information Systems Security Association) with Deloitte, Haskins and Sells. Computer Viruses, Proceedings of an Invitational Symposium. October 1988.

Saita, Anne. Retrospective & Crystal Ball Information Security revisits the voices of the past issues: authors, Interviews and profiles. Information Security Magazine. November 2002.
URL: http://www.infosecuritymag.com/2002/nov/retrospective.shtml#1h (November 22, 2002)

New Hacker's Dictionary. Version 4.3.3. September 20, 2002.
URL: http://www.tuxedo.org/~esr/jargon/jargon.html#virus (November 22, 2002)

Zager, Marsha. Why Hackers Can't Be Stopped. NewsFactor Network. October 31, 2002.
URL: http://www.newsfactor.com/perl/story/19830.html#story-start (November 22, 2002)

VanMeter, Charlene. Defense in depth: A Primer. February 19, 2001.
URL: http://rr.sans.org/start/primer.php (November 22, 2002)

Northcutt, S., Zeltser, Lenny, Winters, Scott, Frederick, Karen, Ritchey, Ronald. Inside Network Perimeter Security. New Riders. 2003.

Postfix. "Postfix Home Page."
URL: http://www.postfix.org/ (November 22, 2002)

Mail-Abuse. "MAPS Realtime Blackhhole List"
URL: http://mail-abuse.org/rbl/ (November 22, 2002)

Practicallynetworked. "Special Application Port List."
URL: http://www.practicallynetworked.com/sharing/app_port_list.htm (November 22, 2002)

von Braun, Joakim.. ID FAQ. SANS.
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm (November 22, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Banes, David. "How to Stay Virus, Worm and Trojan Free - Without Anti-Virus Software." May 16, 2001
URL: http://rr.sans.org/malicious/virus_free.php (November 22, 2002)

SANS." Incident Storm Center."
URL: http://isc.incidents.org/ (November 22, 2002)

NAI. Webshield Appliances.
URL: http://www.mcafeeb2b.com/products/webshield-eapp/default.asp
(November 22, 2002)

Check Point Software. "OPSEC.
URL: http://www.opsec.com/solutions/sec_content_security.html (November 22, 2002)

Finjan. "Finjan Software."
URL: http://www.finjan.com/ (November 22, 2002)

Clearswift. "Clearswift Mimesweeper Suite."
URL: http://www.mimesweeper.com/products/msw/default.asp (November 22, 2002)

Tumbleweed. "Tumbleweed Solutions Products Securemail."
URL: http://www.tumbleweed.com/en/products/solutions/mail.html (November 22, 2002)

ANOMY. "The ANOMY Sanitizer Manual." October 8, 2002.
URL: http://mailtools.anomy.net/sanitizer.html (November 22, 2002)

Trend Micro. "Products."
URL: http://www.trendmicro.com/en/products/global/enterprise.htm (November 22, 2002)

About. "Virus Protection options for Microsoft Exchange and Lotus Notes."
URL: http://antivirus.about.com/cs/groupware/ (November 22, 2002)
Note: I had to use Internet Explorer to get this page to display

Fortinet. "Fortinet."
URL: http://www.fortinet.com/FortiNet/search.jsp (November 22, 2002)

Chau, Jonathan. "Exchange Server Antivirus Software." Windows & .Net Magazine. February 2002.
URL: http://www.secadministrator.com/Files/23564/23564.pdf (November 22, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Demaria, Michael. "InfoExpress CyberGatekeeper Ensures Remote Users Comply With Security Policies." May 13, 2002.
URL: http://www.networkcomputing.com/1310/1310sp3.html (November 22, 2002)

Central Command. "Vexira Antivirus for MailServers."
URL: http://www.centralcommand.com/mailserver_products.html (November 22, 2002)

F-Secure. "F-Secure Virus Information Page: PDF Worm." August 9, 2001.
URL: http://www.europe.f-secure.com/v-descs/pdf.shtml (November 22, 2002)

Pardo, Dani. "A Centralized and Flexible Antivirus Solution."
URL: http://www.samag.com/documents/s=1154/sam0102c/0102c.htm (November 22, 2002)

Symantec. "How to disable or remove the Windows Scripting Host."
URL:
http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html (November 22, 2002)

Security NNOV: Advisories: Content. "Bypassing content filtering whitepaper."
URL: http://www.security.nnov.ru/advisories/content.asp (November 22, 2002)

Symantec." The potential dangers of instant messaging."
URL: http://www.symantec.com/homecomputing/library/i_message.html (November 22, 2002)

Symantec. "Enterprise Solutions."
URL: http://enterprisesecurity.symantec.com/Content/ProductLink.cfm?EID=0 (November 22, 2002)

Symantec. "Antivirus for palm."
URL: http://www.symantec.com/sav/features.html (November 22, 2002)

Central Command. "Vexira Antivirus for Linux."
URL: http://www.centralcommand.com/linux_products.html (November 22, 2002)

ICSA. "Anti-Virus Product Developers Consortium."
URL: http://www.icsalabs.com/html/communities/antivirus/index.shtml November 22, 2002

Gullet, Chris. "Computer Virus Policy, Training, Software Protection and Incident Response for the Medium Sized Organization: A How-To Guide." July 30, 2001
URL: http://rr.sans.org/malicious/medium.php (November 22, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Lubow, Eric.."Sendmail Trojan Looks Familiar." October 11, 2002
URL: http://www.linuxsecurity.com/articles/hackscracks_article-5902.html
(November 22, 2002)

Eicar "eicar Antivirus test file."
URL: http://www.eicar.org/anti_virus_test_file.htm (November 22, 2002)

Lynxwiler, Rodney. "Implementing A Norton Antivirus Managed Infrastructure". March 21, 2002
URL: http://rr.sans.org/malicious/norton.php (November 22, 2002)

Botelho, Andre. "Norton Antivirus C.E 7.6." October 10, 2001
URL: http://rr.sans.org/toppapers/norton.php (November 22, 2002)

Virus Bulletin. "
URL: http://www.virusbtn.com/ (November 22, 2002)

Symantec. "Symantec Security Response – Removal Tools Page."
URL: http://www.symantec.com/avcenter/tools.list.html (November 22, 2002)

McAfee. "AVERT Tools."
URL: http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/tools.asp (November 22, 2002)

Schmehl, Paul. "Holistic Enterprise Anti-Virus Protection." January 21, 2002.
URL: http://online.securityfocus.com/infocus/1538 (November 22, 2002)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced