Best practice for multi-tier virus protection

David Mitchell and Katherine Carr, Sophos, Oxford, UK

June 2002

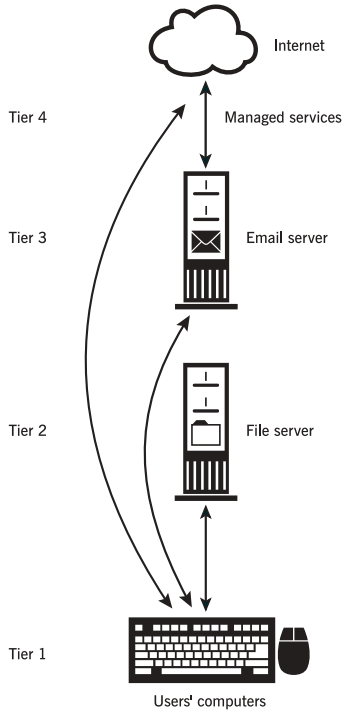
SUMMARY

This white paper describes the different tiers which make up an organisation's IT infrastructure and assesses the need for anti-virus protection at each access point. It also looks at the factors organisations need to take into account when deciding how to manage and where to invest in anti-virus software.

The IT infrastructure

An organisation's IT infrastructure can be seen as having four tiers.

1. **Users' computers**: this tier lies at the heart of an organisation and comprises the individual desktops, laptops and other end-user devices used by all employees.
2. **Local file servers**: this tier lies above the users' computers and contains data and applications which are shared by desktops throughout the organisation.
3. **Email servers**: this tier lies at an organisation's boundary and is the conduit for all email traffic in and out of the organisation.
4. **Managed services**: this is the outermost tier of the IT infrastructure. It can reside inside or outside the organisation but in both cases the software which is being run as part of the service is managed by a third-party, for instance an ISP (Internet Service Provider).



© 2002 Sophos Plc. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

Characteristics of each tier

Tier 1: users' computers

This tier is the most vulnerable area in an organisation since much of the control of the desktop remains with the user. Administrators can "lock down" desktops to some extent, especially under Windows 2000 and Mac OS X but there is much less administrator control possible with Windows 95/98 and earlier versions of Macintosh computers. However what really makes desktops and laptops vulnerable is that this is where all types of data are received - not just from a file server or email server, but also from HTTP-based web traffic, FTP-based file transfers, CD-ROMs, synchronised PDA (Personal Digital Assistant) data and so on.

Users' computers are the most difficult to manage because of the sheer number of machines involved. Indeed, many organisations find it difficult even to know the exact number of machines that exist.

Tier 2: file servers

Most organisations have far fewer file servers than user computers. Administrators have much more control over what is on each server, the abilities of end-users to access the machines being much more effectively regulated. While they can make use of the shared data on these servers, end-users do not have control over the settings. Popular operating systems for file servers include Unix, Windows NT/2000 and NetWare.

Tier 3: email servers

Email servers sit at the gateway and process email traffic entering or leaving an organisation. They support protocols such as SMTP (Simple Mail Transfer Protocol) as well as email products such as Lotus Notes/Domino and Microsoft Exchange.

A survey conducted in January-March 2000 for message managers Pitney Bowes found that the average Fortune 1000 employee was handling 50 emails a day.[1] Large organisations can receive upwards of 50,000 mail messages a day, some getting as many as a million. According to the IDC (International Data Corporation) by 2005 there will be 35 billion emails sent daily.[2] This level of traffic combined with the proliferation of email-aware viruses means that email is now the main route by which viruses enter organisations. Some companies can stop tens or even hundreds of viruses a day at the gateway.

Tier 4: managed services

"Managed services" have grown over the last few years and constitute the least specific of the four IT tiers. Essentially the term refers to a third-party company which bundles a number of features and software into one service or hardware appliance which it then manages on behalf of another organisation. By availing itself of this type of managed service, an organisation is relieved of the administrative overhead of managing the process.

One example of a company offering managed services is that of an ISP (Internet Service Provider). An organisation might choose to have its email routed via the ISP and have the ISP scan it for viruses, spam, porn, etc. The ISP then decides what subsequent action to take, eg whether to forward the mail. The ISP charges the organisation for this service.

Another type of managed service is the hardware device, or "appliance". This is usually a specialised server that sits at the edge of the network and controls the

© 2002 Sophos Plc. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

traffic coming in and out of an organisation. It is self-contained and as well as anti-virus software might contain other software such as a firewall. It is not usually possible for an organisation to add any of its own software to the appliance. These appliances are remotely managed by the company selling the device.

Effectiveness of virus scanning at each tier

Tier 1: users' computers

The desktop/laptop tier is the most important layer at which to scan for viruses. It is only at this tier that one is guaranteed to see all data from all possible sources. It is only here that scanning can take place of files in CD-ROMs, in PDAs as they are synchronised, in floppy disks, etc. Emails and their attachments can be scanned here, so, if for any reason there is no anti-virus software at the gateway or it is not up to date, viruses will still be prevented from infecting the network. HTTP traffic coming from the web can also be scanned at the desktop. (Some companies prefer to put in extra protection for HTTP/FTP traffic, say at the gateway, but when the performance degradation this incurs is balanced against the actual threat, which is low, most prefer to rely on the desktop trapping any virus.)

One other important reason for having anti-virus software at the desktop is that this is the only place where encrypted data, such as that using the SSL (Secure Sockets Layer) protocol for secure internet-based transactions, can be checked. Encrypted files cannot be checked by any anti-virus software until they are decrypted.

The difficulties of scanning at this tier in the IT infrastructure arise from the overall administrative difficulties of managing users' computers. As described earlier, the sheer numbers involved can make the task error-prone. Unless administrator controls are rigorously applied and strictly adhered to, users can tamper with the settings and compromise network security. It is also a truism that anti-virus software is only properly effective if it is kept completely up to date.

Tier 2: file servers

Scanning at the file server tier is much more straightforward because there are generally fewer servers than desktops and they are much easier for an administrator to control.

Until fairly recently many organisations have preferred to rely on scheduled scans at the server, knowing that if an infected file did somehow get on to the server, desktop scanning would prevent it from being opened when a user attempted to access it. However, the emergence of new types of virus like W32/Nimda, a Windows 32 virus which spreads aggressively via network shares as well as email and websites, has made the decision about whether to perform on-access scanning at the server less simple. While some organisations in the past have preferred to use only on-demand and scheduled scanning on servers, the inclusion of on-access scanning is now being viewed as an effective means of receiving early warning of a virus having entered the organisation and of preventing its rapid spread across the network.

The caveat in scanning at the file server tier is that, as described above, not all data will be caught; CD-ROM/ DVD files, HTTP/FTP traffic and so on will go directly to the desktop.

Tier 3: email servers

Since the arrival of the Word macro worm WM97/Melissa in March 1999, the

© 2002 Sophos Plc. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

number of email-aware viruses and worms has soared. High-profile examples include the W32/Magistr virus, Visual Basic Script worms such as the Love Bug (VBS/Loveletter) and VBS/Kakworm, and the Windows 32 worm, W32/Klez. These viruses and worms attempt to spread in several ways but most commonly by sending themselves as an email attachment to some or all the addresses in the recipient's address book. In this way hundreds of thousands of users can be infected in a very short space of time. The speed and numbers involved means that scanning at the gateway is now almost as important as scanning at the desktop.

By scanning at the gateway an organisation can stop the threat before it gets to the desktops. This represents a huge saving in administrator time, the administrator only having to deal with the problem at one place - the email server - not at every desktop. Preventing a virus getting on to the network also saves general downtime in the organisation - the initial outbreak of worms such as the Love Bug have brought organisations' networks to a standstill and crippled business activity. In addition, worms like W32/Sircam have attached documents found on the hard disk and forwarded them, compromising the integrity and confidentiality of organisations' data as well as their reputation.

Gateway anti-virus software will scan emails and their attachments as they enter (and leave) an organisation. Email products will also include mailbox and database scanning, which means that even if viruses have not been detected at the initial real-time scan - for instance if there was a delay in updating the anti-virus software - they will be caught on a subsequent scheduled or on-demand scan.

So for reasons of time, cost and reputation, scanning emails as they enter and leave an organisation is clearly to be recommended. Once again the caveat is that one is not guaranteed to see all the data at the gateway, with user-based media and encrypted mail needing to be scanned at the desktop.

Tier 4: managed services

The significant advantage of using a third-party to manage the process of protecting your data at the boundary is that administrators can spend time on other activities. In addition, the costs involved in implementing protection at this tier are much more predictable than at any of the other tiers.

However, these advantages must be weighed against the potential disadvantage that the whole process is completely outside the organisation's/administrator's control. The organisation is almost completely dependent on the settings, decisions and efficiency of the ISP or other service and if practical problems occur, for instance in network routing, there is little the organisation can do. There are also privacy issues to consider, as this approach means that staff outside the organisation might be able to view data contained in the emails. There might be more control if the service is operated via an appliance, but it is still managed by a third-party.

Choosing an anti-virus solution

In reviewing the factors affecting the choice of anti-virus solution, there is a sliding scale of maximising security versus minimising costs. Protection at tier 4, the managed services, minimises costs; protection at tier 1 maximises security.

It is reasonable to assert that all organisations should be protected at tier 1, at the users' desktops. Policies among anti-virus companies differ but at Sophos, for instance, licences for desktops automatically include file server protection, ie tier 2.

Having protected tiers 1 and 2, organisations might then choose to protect tiers 3

© 2002 Sophos Plc. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

and/or 4 depending on the costs and security issues involved. Implementing anti-virus software at tier 3, the gateway, gives an organisation much more control and better privacy protection. However, outsourcing the task to a managed service provider (at tier 4) might be the preferred solution for an organisation where cost is the overriding factor.

Some organisations prefer to use two suppliers - one for tiers 1 and 2, and another for tiers 3 or 4. In reality all the major anti-virus companies provide the same high levels of detection and there is cooperation amongst them to ensure that this remains the case; the differences between the companies lie rather in the level and quality of support which they offer. The choice of whether to use two different suppliers - like many of the issues discussed in this paper - comes down to a tradeoff. In this case the tradeoff is between the perceived peace of mind of a belt and braces approach and the cost of paying more for two separate products as well as the doubled administrative support overhead.

Sources

1 “Pitney Bowes messaging study highlights differences in communications strategies among workers in small, medium and large businesses”, Press release, 21 August 2000

2 http://one.ie/report/email/marketoverview.asp