

Best practice for multi-tier network security

Sophos, UK
January 2005

SUMMARY

This white paper describes the different tiers which make up an organisation's IT infrastructure and assesses the need for security 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, endpoint and gateway protection.

The IT infrastructure

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

- 1 **Users' computers:** this tier lies at the endpoint of an organisation and comprises the individual desktops, laptops and other end-user devices used by all employees. It also includes the laptops of remote or travelling staff.
- 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 **Gateway/email servers:** this tier lies at an organisation's boundary. It is the conduit for all email traffic in and out of the organisation.

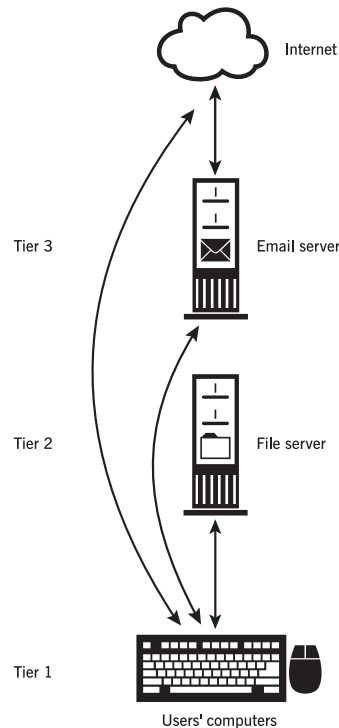


Figure 1: The three tiers of an organisation's IT infrastructure.

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 XP and Mac OS X but there is much less administrator control possible with earlier, still widely used platforms, such as 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 and USB memory sticks, synchronised PDA (Personal Digital Assistant) data and so on. Users' computers can also be vulnerable when linking to unsecured wireless networks, or using hotspots – areas where a wireless internet connection can be accessed by the employees or the public.

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 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. There are several popular operating systems for file servers including Unix, Windows NT/2000/2003/XP and NetWare.

Tier 3: gateway/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 Microsoft Exchange and Lotus Notes/Domino.

The high level of email traffic, the proliferation of email-aware viruses and the increasing collaboration of spammers, hackers and virus writers means that email is now the main route by which viruses and other malware enter organisations. Some companies can stop tens or even hundreds of viruses a day at the gateway, often delivered via spam. The volume of spam sent worldwide is still growing despite attempts to legislate against it in many countries. IDC (International Data Corporation) predicts that the number of spam messages sent daily will reach 23 billion by 2007.¹

Email is now the most common method by which viruses, malicious spyware and worms spread.

Effectiveness of protection at each tier

Tier 1: users' computers

The desktop/laptop tier is arguably the most important layer at which to scan for viruses and spyware. Although most of today's rapidly spreading viruses spread via email, not all viruses are email-borne. For example, the Sasser worm (one of the most prevalent of 2004) is not. Neither were the second and third most reported viruses in 2003 – Blaster and Nachi. Many viruses are now blended threats, spreading in more than one way, for example by network shares as well as email. It is only at the desktop/laptop tier that data from all possible sources is guaranteed to be scanned. There are many possible sources of infection as described on the previous page. Emails and their attachments can be scanned at

the user's computer 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.

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 number of viruses spreading in ways other than email, such as via network shares, means protection of the endpoint (file servers and desktops) is still vital to organisations.

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. By scanning file servers, anti-virus software is an effective means of receiving early warning of a virus like the those in the Netsky family, which can spread aggressively within an organisation via network shares as well as email and websites. 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: gateway/email server

The email gateway of an organisation represents an increasingly complex and varied threat environment. Spam, phishing attacks, Trojans, viruses and worms are all able to infiltrate a company's IT infrastructure via email, whether individually or, increasingly, as a combination of threats. This trend is reflected in the convergence of spam and virus threats – the success of spam has brought hackers, virus writers and spammers together in an underground economy based on unsolicited email. Since the arrival of the Word macro worm WM97/Melissa in March 1999, the number of email-aware viruses and worms has soared, with high-profile examples including MyDoom and Bagle. These viruses and worms attempt to spread in several ways, but most commonly by sending themselves as an email attachment to some or all of 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.

Using software that scans for all varieties of threat at the gateway brings several advantages. By stopping viruses and spam before they enter the corporate network and reach employees, network and administration resources are saved, as well as preventing loss of productivity. Employees are also shielded from offensive spam and frauds such as phishing. Gateway anti-virus software will scan emails and their attachments as they enter (and leave) an organisation. However, products such as Sophos PureMessage 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, resources, crime prevention, cost and reputation, scanning emails as they enter and leave an organisation is important. 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.

The variety and complexity of threats make the protection of both the endpoint and gateway of a network vital.

Choosing the right protection

Security threats to corporate networks are growing in terms of their numbers, speed of delivery, and the variety of ways in which they can combine. This makes protection for businesses an ever more complex problem that can only be addressed by protecting all entry points to a network. Implementing a consolidated solution which provides both gateway/email server and endpoint protection is the best way to guard organisations in an increasingly complex threat environment.

Sophos Anti-Virus, SAV Interface and Sophos PureMessage together provide an integrated, total solution, managing the complexities of corporate IT infrastructures in companies of any size and across many different platforms. They are backed by 24-hour support, a worldwide threat detection network and a global system of research labs providing expert analysis and rapid response to the latest threats. Although all major anti-virus companies provide high levels of detection and there is cooperation amongst them to ensure that this remains the case, the differences between the companies lie in the level and quality of support which they offer, and in the complexity and depth of protection they provide.

Sources

- 1 IDC – "Worldwide Secure Content Management 2004-2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security", by Brian E Burke.