

Protecting small and growing businesses

A Sophos positioning paper

October 2006

Viruses and other security threats have developed into sophisticated tools in the hands of cybercriminals. The effect of a malware attack, particularly on a small business, can be highly disruptive or even catastrophic, since it is often smaller companies that lack the time and IT resources to devote to network security. This paper describes the evolving threat, provides best practice advice on protecting computers, and outlines the ways in which Sophos small business solutions meet the specific needs of small businesses for reliable, integrated protection.

The threat to business continuity

All organizations, regardless of size, are at risk of disruption or damage from security threats. However, smaller businesses face several unique security challenges:

- IT is not necessarily a dedicated role.
- The organization has fewer, or limited, IT skills compared with larger corporations.
- There is little time to consider IT issues beyond immediate day-to-day needs. This can lead to security not being given the priority that may be required.

Network downtime, lost productivity and loss of confidential information can have a critical effect on smaller enterprises, which cannot afford the resulting losses or business disruption. The threats facing businesses can be divided into three main categories: malware, hackers, and productivity drains.

Malware includes viruses, spyware, Trojans, and any other piece of malicious code. Hackers threaten security by breaking into computer systems, often using malware to do so, and using them for a variety of criminal purposes, from storing pirated software to sending out spam. Productivity drains need not be malicious, but can still be undesirable or time-wasting. Examples include spam and adware – applications which install themselves on a user's computer, and then display advertising banners and pop-ups on the desktop. While not classed as malicious, adware disrupts user productivity and slows computers.

The challenge of the accelerating threat

The threat to business has changed enormously since the emergence of the first PC virus, Brain, in 1986. The arrival of the first email-aware viruses – Melissa in 1999 and the Love Bug in 2000 – vastly increased the speed at which

companies could be infected. Since then, the threat has continued to increase in terms of the sheer number of viruses, the speed at which they spread, and the overall complexity of the problem.

Quantity

The total number of viruses has continued to multiply at rates originally believed to be unsustainable. Sophos Anti-Virus now identifies around 200,000 different threats, and the number is constantly rising. SophosLabs™ – a global network of threat analysis centers – sees over 4,000 new viruses every month. Although direct viral attacks via email are declining, collaboration between virus writers and spammers is resulting in more effective and targeted delivery of malware.

Sophos Anti-Virus now identifies around 200,000 different threats – the number is constantly rising and threats are becoming more targeted.

Velocity

The speed at which new attacks spread is also increasing. Internet worms like Sasser and Zotob, which exploited security vulnerabilities or loopholes in Windows operating systems or Windows applications, can infect hundreds of thousands of computers worldwide within minutes. Meanwhile, insufficiently protected computers are coming under attack in shorter timescales than ever before. Figure 1 illustrates how quickly a vulnerable desktop can be infected – Sophos research shows that connecting an unprotected, unpatched computer running Windows XP (without SP2) to the internet leads to a 50% risk of infection within 30 minutes, rising to a probability of almost 75% after 60 minutes. There may not even be time to download and install patches or firewalls.

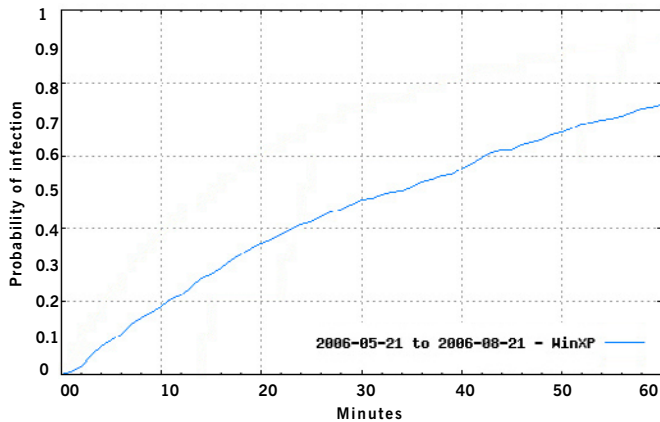


Figure 1: Probability of infection of an unprotected computer running Windows XP connected to the internet.

Complexity

The problem of securing business networks is becoming increasingly complex as IT systems become more intricate, with networks more likely to include laptops that are taken in and out of the office. Security threats have also become more complex and targeted in recent years. The main drivers are money and maintaining a low profile – virus writers and spammers are joining forces to use malicious code with the aim of stealing money or information, without drawing unnecessary attention to themselves. Examples include Trojan horses that steal bank account details, and dialers which secretly connect an infected PC to a premium rate phone service, running up large bills. Today, many virus attacks are the work of organized gangs of criminals. The financial motive has led to the development of a profusion of new types of increasingly complex threat. These can spread in a variety of ways, often blending characteristics of viruses, worms, spyware, and spam. Spyware and phishing are two of the biggest threats that businesses now face, and malware attacks are almost universally targeted on a small number of victims compared to the mass-mailing worms of the past, in an attempt to avoid the sort of publicity that will increase the probability of users taking steps to protect themselves.

Best practice advice

There are some simple measures which small businesses can take to avoid being damaged by viruses and other security threats. Detailed information can be found on the Sophos website¹.

Make all staff aware of the risks

Many virus attacks and cybercrimes rely on psychological tricks to dupe users into activating malicious code, for example by

opening an attachment in an email. Unsophisticated computer users are particularly vulnerable, so educating employees in best practice can significantly improve security. Businesses should implement an anti-virus policy, including a procedure for vetting media such as CDs and USB sticks brought into the office by employees. Similarly, a policy should be established specifying which file types are safe to be downloaded from the internet. Equally important is the message that all emails should be treated with caution, as viral emails might appear to come from colleagues or friends. The education process should be ongoing to ensure everyone is kept up to date.

Install anti-virus software and update it regularly

If malware does infiltrate a business, it is vital that it is stopped before it can spread throughout the company network. Anti-virus solutions use on-access virus scanning, which checks for viruses in real time as a file is opened. If the file contains a virus, spyware, or other malware, access to it is blocked, stopping the malware from spreading. It is essential that anti-virus software is regularly updated with protection from the latest malware, as new variants emerge every day. The best way to make sure that anti-virus protection is kept up to date is to use a solution which updates itself automatically, enabling the software to be set up and left to run without supervision.

Use software patches to close security loopholes

Many viruses and other malware spread by using loopholes or security vulnerabilities within operating systems and common applications, such as web browsers. As well as using anti-virus and anti-spyware solutions, businesses need to update their systems to close security loopholes. This can be done by installing software patches, which vendors such as Microsoft release whenever a vulnerability is discovered. Vendors publish regular updates giving details of what new patches are recommended. It is also possible to get automatic updates from vendor websites, making it easier to stay up to date.

As well as using anti-malware solutions, businesses need to update their systems to close security loopholes.

Keep on top of new threats

New and blended threats are always emerging, and it pays to keep abreast of developments. Businesses can sign up to a variety of alert services, such as the free email alert service from Sophos, which can be subscribed to from the Sophos website. Alert services provide early warnings of new threats, and allow administrators to check whether their anti-virus and anti-spam protection is adequate.

Use client firewalls

Client firewalls control which applications are allowed to send information over the internet – this stops malware such as Trojan horses infecting computers and using them to steal information. In addition, client firewalls protect against internet and network worms, using port blocking to prevent the malware from gaining access.

A third function of client firewalls is to hide computers from other computers on the internet, which may be used by hackers. Hackers use port scanning to find computers they can break into – sending out random messages over the internet and waiting for replies from vulnerable computers. Using a desktop or client firewall ensures that the computer does not reply to the hackers’ messages, making it less vulnerable.

Keep backups of all data

It is important to prepare in case the worst should happen and a virus causes damage to a business’s computers or data. Restoring data from backups remains the best way to recover from a virus attack – all important or business-critical information should be backed up and stored separately.

It is important to prepare in case the worst should happen and a virus causes damage to a business’s computers or data.

Choosing a security solution

In assessing the cost-effectiveness of a network security product and evaluating the total cost of ownership (TCO), price is just one consideration. Other factors include:

- Ease of use
- Speed of response
- Protection against unknown threats
- Support.

Ease of use and technical support are particularly crucial to smaller organizations, minimizing administration and leaving them free to concentrate on core business activities, knowing that their IT systems are protected.

Ease of use

Small business customers are often frustrated with their security solutions, due to the complexity of multiple packages and management tools, difficulties with initial configuration, and ongoing management. Security software must be easy to

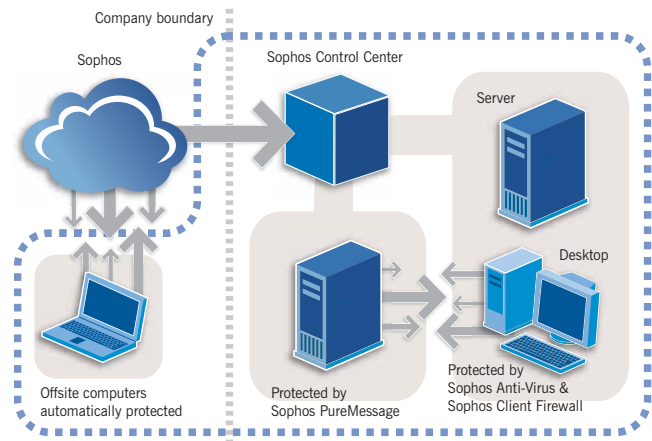


Figure 2: How Sophos small business solutions provide networks with all-points protection

install, configure, and update, either automatically or with little effort. Sophos Security Suite is specifically designed for non-technical users and provides comprehensive protection against multiple threats in a single product. It is simple and easy to set up and can be deployed across the entire network from a single location in a matter of minutes. Figure 2 shows how all parts of the network are protected.

The straightforward user interface enables any user to install and manage the software quickly and easily. All regular tasks such as deploying protection to new computers are made simple. Sophos Control Center, illustrated in Figure 3, gives an overview of the status of every Windows computer on the network. This allows unprotected or new computers to be identified easily and virus alerts to be monitored.

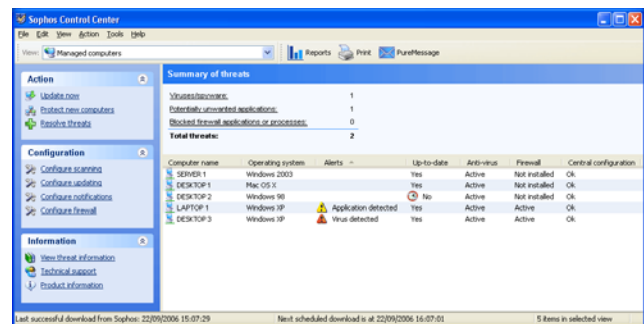


Figure 3: The Sophos Control Center

Policies for scanning email for viruses and spam can be set using the Sophos PureMessage Console. For example, spam rules can be set to determine whether suspect messages are deleted or quarantined. Allow lists (lists of clean senders) and block lists (lists of known spammers’ servers) can also be used to improve message filtering.

Speed of response

SophosLabs keeps a 24/7 watch on new malware and spam campaigns, applying expert analysis to millions of emails a day. The cross-threat expertise in SophosLabs, and its agility in responding to new campaigns, make Sophos uniquely able to integrate the management of all threats, no matter how they spread. Sophos regularly tops the rankings of global security vendors for average speed in responding to new threats². The service Sophos provides to small and growing businesses is no different from that delivered to large corporate, government and education establishments.

Protection against unknown threats

Sophos Anti-Virus and Sophos PureMessage have won many awards for consistently high detection rates and robust performance, but a high detection rate for viruses and spam, while essential, is not sufficient today. Unknown and so-called day zero threats – those that can execute before specific protection is released – are an increasing risk to business. To combat this problem, Sophos solutions employ Genotype[®] detection technology, which provides proactive protection against new variants of viruses and spam campaigns.

Behavioral Genotype Protection, included in Sophos Security Suite, takes this one step further: it identifies and blocks malicious code before it can execute. This technology improves on the benefits of most Host Intrusion Prevention Systems (HIPS), which are runtime solutions that allow the code to begin execution before stopping it – increasing the risk of damage. Sophos Client Firewall™ – also included in Sophos Security Suite – proactively locks down computers, safeguarding against internet worms, hackers, and the risk of unprotected computers connecting to and infecting a network.

1 www.sophos.com/security/best-practice/

2 www.av-test.org/

About Sophos

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

Support

Sophos support is provided round the clock to all customers at no additional cost to the license purchase. Sophos support comes from a dedicated, locally based, in-house team of experts who can offer practical detailed knowledge and experience, which has resulted in the highest levels of customer satisfaction in the industry.

Maximize peace of mind, minimize costs

Sophos Security Suite keeps itself up to date so that users are always protected from the latest threats. Sophos AutoUpdate checks 24 hours a day for the latest virus and spam updates from SophosLabs, automatically delivering and deploying them to each computer on the network.

The automated, simple-to-manage functions of Sophos Security Suite enable organizations to concentrate on their core business activities, safe in the knowledge that their network is protected by an integrated and complete solution that is trusted by over 35 million business users worldwide.

Conclusion

The threat landscape is continually evolving, with viruses, spyware, Trojans, phishing, and spam merging to form new, faster-moving, targeted threats. Small and growing businesses need a security solution which provides reliable, cost-effective protection with a minimum of time investment.

Sophos Security Suite, backed by SophosLabs, fills the security gap caused by lack of IT resources and expertise in smaller businesses, providing security and peace of mind.