SOPHOS

Top five strategies for combating modern threats

Is anti-virus dead?

Today's fast, targeted, silent threats take advantage of the open network and new technologies that support an increasingly mobile workforce. Organizations need innovative approaches to protect the web, email servers and endpoint. This paper discusses the security implications of modern threats, analyzes where emerging technologies can add real value, and highlights five key strategies for ensuring solid malware protection.

A Sophos white paper

October 2008

Top five strategies for combating modern threats: Is anti-virus dead?

Changing environment and threat

The corporate IT environment has changed irrevocably over the last few years.

Threats are no longer high-profile viruses that spread themselves obviously to millions of internet users for maximum publicity. Now they are highly targeted, silently infecting computers to steal data and make money for criminals. They are increasingly surreptitious and low profile, mutating in hours or even minutes to evade detection.

At the same time, today's working environment is rapidly changing. The network perimeter has dissolved to such an extent that it is virtually unidentifiable. Yesterday's "castle and moat" architecture – with its office-based desktops and servers protected by a gateway firewall – has crumbled. Remote working, the use of endpoint devices such as USB sticks, constant internet access and the rapid emergence of Web 2.0 technologies have redefined how employees interact with an organization's systems. In addition, increasingly complex networks must accommodate not just employees, but also outside contractors, vendors and customers.

The need for all points protection

Cybercriminals exploit any vulnerability they can find to infect corporate networks. Their latest tricks use countless loopholes in web security to get malware onto a user's computer in seconds. One new infected webpage is discovered every five seconds, and over 90 percent of these pages are on legitimate websites that have been compromised.

Users are duped into visiting these compromised websites, typically via links in spammed emails. There can be layers of complexity with the original website going to another site and that in turn going to a third, and so on, ending with a Trojan being downloaded onto the user's computer – all of this happening in a matter of seconds.

The task of securing the network against this and other exploits – at the web, email and endpoint – is a daunting challenge for today's IT departments who are being asked to do more and more with their constrained budgets.

Anatomy of a threat

Here is how a significant number of infections are achieved:

- As part of a highly targeted spam campaign, a user gets an email from a hijacked computer.
- The spammed email includes nothing more than a subject line and a link to an infected website.
- This is a legitimate site so the user is not suspicious and clicks on the link.
- Using a vulnerability to install, a Trojan is immediately downloaded onto their computer.
- Their computer sends confidential data to the hacker.
- The hacker also uses the newly hijacked computer to send out more spam campaigns.

Reducing the attack surface

Within this new threat environment, and as attitudes to work and information continue to evolve away from those of the past, organizations have become more aware of the acute need to control all points on the network to protect its data and systems from criminals. However, the speed with which new threats emerge and infect means that defenses are often inadequate and usually out of date.

Protection versus detection

While much can be achieved by user education and enforcement of acceptable use policies – for example, banning unencrypted laptops and USBs from being taken out of the office, or stipulating what can and cannot be sent by email[1] – there is need to take a different approach to technology in order to reduce the attack surface and protect the network, systems and data from malware.

In addition to the ability to detect, there are several criteria that need to be taken into account to ensure ongoing manageable protection. The key strategies are highlighted below.

STRATEGY 1

Maintain traditional anti-virus protection

Totally reliable malware detection remains at the core of any security solution, and updates created by security vendors from samples of particular viruses still form the basis of efficient detection.

Issues of manageability and automation are important – anti-virus will only protect the network if it is correctly configured, deployed and updated across the whole network, and new computers logging on to the network need to have anti-virus software installed immediately and automatically.

So while organizations need to take other approaches into account too and use other technologies, powerful traditional anti-virus protection remains crucial. It is relying **solely** on the traditional reactive approach that is no longer adequate.

STRATEGY 2

Proactively protect the network

Traditionally, protection against malware and spam was created by security vendors collecting samples of particular viruses and spam, and then developing specific protection. Today this method is simply too slow and inadequate – there are too many targeted threats and they mutate too rapidly. For example, SophosLabs sees over 20,000 new malicious samples every day. Such large volumes of rapidly mutating malware require proactive, zero-day protection, to protect against threats that the vendor has not yet seen or analyzed.

This proactive protection can be achieved through behavioral analysis, a HIPS-like* technology that aims to stop malware before a specific detection update is released, by monitoring the behavior of code – not just when code is run, but also beforehand:

- Pre-execution analysis – examines the behavior and characteristics of files before the file is run to find traits commonly found in malware.
- Runtime protection – analyzes the behavior of files and processes as they are running, checking for suspicious activity.

An added advantage of strong proactive protection is that the number of individual threats that a research lab needs to analyze is reduced, enabling the rapid creation of new updates and protection where necessary.

STRATEGY 3

Use preventive protection

Network access control

A key weapon in exercising control to ensure security and productivity, is the assessment and management of network access. Finely controlled network access reduces the risk of infection by ensuring security policy is being complied with by all computers – not just those owned and managed routinely by the company but also those unmanaged guest computers connecting to the network.

By assessing and certifying systems before and after they connect to the network, network access control software can ensure compliance with policies, such as requiring all computers to have security software in place and properly configured, and operating system and application patches up to date. In this way organizations can enable safe access to the network, rather than simply blocking guests or maintain hugely inefficient pools of computers for contractors and partners to use.

Safe, effective web browsing

The need to control unauthorized endpoint access to the network is matched by the need to enable safe web browsing while preventing access to infected or inappropriate sites. Although the web has now become the key vector for online hacking attacks, as well as representing a drain on productivity for many businesses, the vast majority of businesses are unprotected against today's modern web-based malware.

Solutions that offer reputation filtering, that is, that block websites known to be "bad", provide some protection, but this is inadequate against "good" sites that have been hacked. Today's threats require that the content itself is also checked – and all this without adversely impacting speed and efficiency.

STRATEGY 4

Control legitimate applications and behavior

Application control

Employees installing and using legitimate but unauthorized applications – such as Instant Messaging, VoIP, games, peer-to-peer file-sharing software, virtualization software, and unapproved browsers – are a real and growing threat. Not only can they introduce malware to the corporate network but they also seriously impact network and employee productivity and cause unnecessary support issues, and further security (and legal) risk if sensitive company or personal data is sent outside the company.

Restricting the use of these non-business-critical software applications narrows the threat vectors and is an increasingly important facet of an overall security policy. For maximum efficiency and return on investment it needs to be incorporated into the management and control features of an organization's anti-malware solution.

* HIPS = Host Intrusion Prevention System

Application whitelisting

Application whitelisting has been suggested as the modern solution to the challenge of protecting computers from unauthorized and malicious software. In this approach, known "good" applications form a whitelist and only this authorized software is allowed to run, in contrast to the traditional approach where "bad" applications (malware) are prevented from running.

The theory is that with application whitelisting, organizations do not need to rely on anti-virus companies to keep up with all the new malware released every day. While the approach has some merit, in reality it is just one of many technologies – such as anti-virus, HIPS and application control that need to be used to ensure comprehensive endpoint security.

STRATEGY 5

Control and encrypt devices and data

The protection of sensitive corporate data, especially in mobile computing, is more important than ever. The news is filled seemingly daily with reports of company laptops, CDs and USB keys packed with confidential information falling into the wrong hands. By using device control you can prevent data being copied and stored on devices like these. However, the problem is that modern business practice often requires the use of such devices. An effective solution to this obvious security weak spot is encryption to ensure that, though the medium might be lost, the data itself is protected and that no unauthorized person can access it or the rest of their IT infrastructure.

By encrypting the entire contents of a hard drive, organizations can complement the operating system's own mechanisms and safeguard the computer's operating system along with its data, ensuring that no changes or unauthorized access can be made.

Is application whitelisting the magic bullet?

Application whitelisting – allowing only known "good" applications to run has both strengths and weaknesses as a solution to the problem of today's threats.

Strengths

- A strategy which allows only good code to run is a very appealing concept.
- Whitelisting is a valuable approach for locked-down parts of organizations, where there are already strong restrictions on what applications can be used and where those applications rarely change, for example Point of Sale (POS) terminals in retail outlets, or servers performing a limited, core set of functions.

Weaknesses

- Application whitelisting does not deal with types of malware that depend on subverting known good applications, including script malware running in browsers, macro viruses in Office, buffer overflows.
- If malware evades detection by a whitelisting solution, cleaning up the infection is a major task.
- The whitelisting vendor has to keep up with every release of a good application, as well as custom applications.
- Administrators need to know exactly what they want to allow in order to define policy and have to maintain at least some of the whitelist themselves.
- When the policy is defined, there is still a major challenge in identifying and maintaining the list of authorized applications, without impacting user or IT staff productivity.

Encryption can also help avoid statutory public disclosure requirements and limit the liability associated with a data leakage incident as many data protection laws have been updated to accept appropriate encryption as an acceptable safeguard.

Strategy support through vendor expertise

Underpinning the technology of any solution is the vendor's expertise, experience and understanding of the threat environment. The beginning of this paper demonstrated the complexity and blended nature of today's threats. A vendor with truly integrated visibility of spam, virus and web-based threats will be able to ensure the rapid response needed to combat new threats. In addition, just as analysis needs to reach across all threat types and technologies, so does the support offered by help teams.

Conclusion

Although traditional anti-virus protection remains the cornerstone of reliable security, modern threats require solutions that go beyond this, providing proactive protection against fast-moving, zero-day malware. The wider issues of controlling network access, web browsing and applications need to be addressed by organizations as a matter of urgency, and the importance of encryption in securing corporate data needs to be understood and acted upon. Finally, organizations need to ensure that their vendor has the cross-threat expertise both in its labs and in its support teams, to make the solution cost-effective and successful.

Sophos solution

Sophos solutions provide proactive protection at the web, email and endpoint through Behavioral Genotype™ Protection (HIPS). Application and device control and Sophos NAC in Sophos Endpoint Security and Control provide extra security and control on desktops and laptops, while Sophos Web Security and Control provides reputation and content filtering and also detection of the anonymizing proxies used to bypass traditional filters. Sophos Email Security and Control is enhanced by SXL (Sophos eXtensible Lists) which delivers spam updates in real time. All our products are backed up by cross-threat expertise and automated systems in SophosLabs and 24/7 technical support.

Sources

1 You can find useful guidance on creating an acceptable use policy in "Stopping data leakage: exploiting your existing security investment", www.sophos.com/sophos/docs/eng/papers/sophos-dlp-wpna.pdf

and in

"Effective email policies:Why enforcing proper use is critical to security", www.sophos.com/sophos/docs/eng/papers/sophos-email-acceptable-use-policies-wpna.pdf

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM