Four principles of effective threat protection:

Defining the right strategy and tools to defend your business against malware

With all the web-connected ways your organization does business, you have to be ready to handle malware attacks, multiplying threat vectors and increased compliance responsibilities. Threat protection requires an updated approach now that the classic model of anti-virus plus firewall is no longer enough. Current best practice calls for interlocking layers of protection that support your company's business processes and the digital assets you need to protect. This paper describes principles you can use to strike the best balance between enabling your business and ensuring effective security.

by Shai Gelbaum, Product Manager, Sophos

A Sophos white paper

May 2010

Four principles of effective threat protection: Defining the right strategy and tools to defend your business against malware

A business challenge

Digital business has become a mainstay as internet-based technology and services have become vastly more affordable and easier to use. Today your organization is able to support your business processes with tools that include web storefronts, social networking and software as a service (SaaS), whether you work in a small or medium-sized business (SMB) or a large corporation.

The trouble is that criminals have targeted the web-connected technologies that serve reputable businesses so well. Cybercriminals use malware, or malicious software, including viruses, worms, Trojan horses and spyware to exploit any vulnerability they find. Using this malicious software to penetrate weak defenses, criminals steal valuable data and commandeer computer processing that they sell on a global black market.

Malware attacks present a danger that cannot be ignored. (**See the sidebar, The threat landscape.**) Much is at risk: the costs of security breaches, the continuity of your business and your organization's compliance with regulations. And you face these same consequences and responsibilities no matter what size your business is.

What security breaches cost

The costs are often substantial when an attacker compromises your IT systems or gains access to your data. Consider that data does not even have to be stolen in a breach to trigger notification requirements and other expensive fallout. If you do not stop an intrusion into your computer systems and your data is not encrypted, regulations may obligate you to report the incident to every individual whose personal data might have been exposed.

Annual studies measure the damage in financial terms:

- The CSI Computer Crime and Security Survey 2009[1] found average losses due to security incidents of all types were $234,244 per respondent. The figure declined from $289,000 per respondent in 2008, but was higher than in 2005 and 2006. Financial fraud costs rose in 2009 to approximately $450,000 per incident, according to the Computer Security Institute study.
- According to the Ponemon Institute's fifth annual U.S. Cost of a Data Breach Study released in January 2010, the average cost of a data breach in 2009 was $204 per record compromised[2]. The average total cost per reporting company exceeded $6.75 million per breach. The cost ranged from $750,000 to almost $31 million.

The threat to business continuity

Security breaches affect businesses in ways that interfere with your ability to use your systems, your data or both—resulting in more time and money lost. For instance, PCs that become infected with malware must be quarantined for cleanup. The users of those PCs are unable to do their normal work during that time. You also have the expense of hiring a technical professional to do the remediation.

Or perhaps a malware infection causes your organization to lose access to customer records stored on a hard drive. Will you be able to recover that data? How long will recovery take? In the meantime, your company can't process orders and answer customer service questions.

Regulatory and compliance risk

Besides the costs related to a security breach, businesses are responsible for complying with a growing body of government regulations and industry standards related to data privacy and security. Regardless of the size of your organization, you have to play by the rules. Non-compliance with the following regulations leaves you at risk of penalties that tarnish your company's reputation and could put you out of business:

National and state regulations covering citizen data:

Laws currently on the books include a regulation that went into effect on March 1, 2010 in the state of Massachusetts. With implications beyond the state's borders, 201 CMR 17.00 requires any company that conducts business with Massachusetts residents to implement a comprehensive data security plan that covers personal information in paper and electronic forms[3].

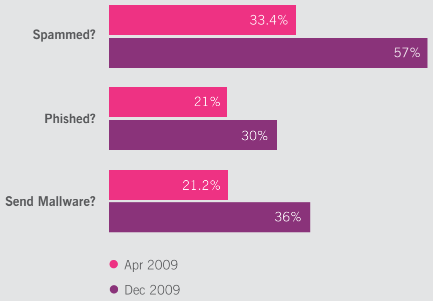
4

The threat landscape

Cybercriminals mount their often stealthy attacks using malware to infect computers through unpatched security holes in software and any other weakness they uncover. The Security Threat Report: 2010[4] by Sophos found that criminals are taking advantage of both old and new vulnerabilities:

Social network use by businesses, customers and employees: Businesses eager to connect with their customers and communities have flocked to social networking sites, including Facebook and Twitter. Sophos found a 70% rise in the proportion of firms that say they encountered spam and malware attacks via social networks during 2009. More than half of all companies surveyed said they had received spam via social networking sites, and over a third said they had received malware.

On social networks, have you ever been?



Infected webpages: The web remains the number one vehicle for malware used to infect computers and steal data. Not only do malicious sites put visitors at risk, but legitimate sites are also being hijacked by criminals to host their wares. The danger here is high because visitors trust the popups and inserts they find on legitimate websites.

Email and IM spam: Spam continues to be an important vector for the spread of malware, delivering a malicious payload to recipients either through a file attached to the spam message or by embedding a link to an infected website. Criminals today use both traditional email and instant messages (IMs) in their spam campaigns.
The numbers show that spam is an enormous threat. Sophos research reveals that 89.7% of all business email is spam. SophosLabs also identifies approximately 6,500 new spam-related webpages every day, or one new website every 13 seconds, 24 hours a day. This figure almost doubled from the same period of 2008 (one every 20 seconds).

PCI DSS:

The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization or retailer that accepts payment card transactions, or that collects, processes or stores credit card transaction information. Sanctions for non-compliance range from fines to being disqualified from credit card programs[5].

HIPAA:

The scope of the U.S. Health Insurance Portability and Accountability Act (HIPAA) has been extended by the HITECH Act, which broadens compliance obligations to include the business associates of HIPAA-covered entities. Stronger penalties allow a covered organization to be fined up to $1,500,000 per calendar year for each violation of the personal health information guidelines[6].

A new model for threat protection

A successful protection strategy has to support the way you do business today, and must prepare your organization to respond to a growing number of organized attacks, threat vectors and compliance responsibilities.

There was a time when users accessed data and applications only from desktop PCs on your company's internal network. The line between the inside and the outside of your organization was clear. Back then, the accepted model for threat protection was to load anti-virus software on your endpoint PCs and put a firewall around your internal network. Mobile users and the rise of cloud-based services, such as Amazon.com web storefronts and Salesforce.com CRM, have caused that line to blur.

Effective threat protection requires more than anti-virus and firewall software. Organizations are adding more layers of safeguards such as web filtering and spam protection, particularly at endpoints where users access the internet.

The objective of threat protection is making sure your business functions without being affected by security breaches and malware. Effective security will enable your business model and allow users to work productively, without getting in the way.

Four principles—prevention, proactiveness, performance and simplicity—form a basis for the new threat protection strategy. You can use these principles to guide you in implementing the layers of security you need to support web-enabled business processes.

Prevention

Because the barrage of new threats is constant, securing your IT environment means prevention first. SophosLabs detects a newly infected web page on the internet about once every four seconds. In 2009, SophosLabs received 50,000 new malware samples every day[7].

Successful prevention depends on interlocking layers of protection. To define the right security policies and choose the right measures to enforce them, think about how you do business and the nature of the assets you need to protect. You may need to secure an internal order system that is visible to the ecommerce provider where your customers make their purchases. Or you may have to control access to data that is a critical asset, or enforce the allowable use and handling of data as permitted by law.

Some elements are necessary for any organization, including web filtering, email filtering, firewalls and anti-virus software on endpoint PCs. Third-party connections to your important business systems and sensitive data call for strong authentication and data encryption. How you implement these and other preventive steps, such as network access control, application control and device control, should be guided by your organization's needs. (See **Interlocking Layers of Threat Protection** for details.)

Proactiveness

You also need the ability to counter any attacks that do get through your outer defenses. Hackers use zero-day exploits to take advantage of vulnerabilities that software vendors are unaware of and have not patched yet. Because a zero-day threat has not been encountered before, there is no characteristic signature for security software to detect. One type of exploit that tries to defeat malware analysis is the polymorphing threat, in which the malicious code changes with every page load.

Host-based intrusion prevention systems (HIPSs) and buffer overflow protection systems (BOPSs) guard against unknown threats that include zero-day exploits. Anti-malware uses these behavior-based detection methods to detect and stop executable code from performing suspicious actions, such as writing to your operating system's driver folder.

Another proactive defense technique is cloud-based reputation systems, including live anti-virus, which check suspicious data online in real time to detect threats. As new threats are discovered, these systems are updated to provide anti-malware signatures on the fly for the timeliest protection possible. Using in-the-cloud protection assumes your computers are connected to the internet so that the checking can take place.

Performance

User experience should be a guiding performance consideration because users find ways to bypass security measures when threat protection gets in the way of their jobs.

A practical guideline is to balance the security your organization requires with the performance that users expect. You don't want users to perceive slow performance that will lead them to turn off security software on their PCs, opening the door to malware infections and attacks.

Also make sure security policy supports how your users work, in addition to enabling your company's business model. Users in your call center might be unnecessarily frustrated by a password policy that requires entering a 14-digit key every 20 minutes. But the same protection could be appropriate for users with access to sensitive data, such as a banker handling financial accounts, or a doctor accessing patients' health records.

Simplicity

Threat protection must be manageable in order to be effective. Keeping things simple also helps you protect your endpoints, users and data without spending more time and money than necessary. You will increase your success in setting up security policy and managing the technology when you:

» **Understand the incremental benefit over the security already in place.** When you consider bringing in any new technology, examine how proposed additions will improve current protection, enable your business processes and strengthen compliance with data security rules.

» **Assess the effect of proposed threat protection measures in your organization.** On the business side, consider whether the security will be too restrictive for your business model and end users. On the technology side, determine whether you have the technical skills onboard and if upgrades to existing hardware and software are needed.

- **Do as much as you can with the smallest number of products.** Using fewer products reduces the costs associated with software licensing, product installation, ongoing maintenance and overhead on end users' systems.
- **Avoid products that require an expert to manage.** Your organization cannot afford to have highly qualified security engineers spending their valuable hours on tasks that could be automated, or handled by a less specialized staff member. Look for a vendor that offers not just the tools but also the specialist help to maintain and configure protection so that you don't have to invest in costly and rare threat expertise.
- **Account for the cost of maintaining security products.** Examine what manpower is required to manage and update the security products, and whether your staff needs additional training. Unified security products provide an advantage by being easier to manage.

Interlocking layers of threat protection

Starting with the four principles of threat protection will help you balance the proper security with web-enabling your business. Next, you need to look at specific technologies to protect your IT systems and data from being compromised. Let your company's business processes and digital assets be your guides in deciding which layers of threat protection to use, and how to use them best.

Keep in mind that no single technology is a silver bullet; a combination of techniques that "interlock and block" is required for effectiveness. Again, using fewer products or a unified solution to provide the safeguards you need reduces the overhead related to cost, performance and management.

Web filtering

Screening sites with web filtering is recommended for every organization because the web is the leading vector for spreading malware. You can use web filtering to block malware, spyware and phishing; anonymize proxies; and enable use policies for safe web browsing.

Web filtering is essential because users have no way to know when they are visiting a compromised website. Malicious code on the webpage is invisible but executes when the page loads in the user's browser. Typically the code will use cross-site scripting to retrieve a more dangerous payload from a third-party site, which then tries to leverage a vulnerability in the browser or operating system to plant malware, control the computer remotely (to use in a botnet, or a network of compromised computers) or steal data.

You will have a security gap if you only provide web filtering at the perimeter of your network. It is necessary to perform web filtering on endpoint PCs as well. Users do not always go through the company network, for example, to access the internet when they work from home.

Email filtering

Malware continues to infiltrate companies through spam campaigns. Email filtering provides users clean email free of spam and malware by applying the techniques of reputation, content and behavior analysis. Filtering also reduces the time that users spend to weed spam out of their inboxes.

Like web filtering, email filtering is recommended for every organization. Your options include using anti-spam software to filter email on your gateway server, or using an email service provider that filters email for you.

Network access control (NAC)

You can use NAC to check for policy compliance before allowing any computer to access your network. Compliance requirements include being current with anti-virus updates and the latest operating system patches.

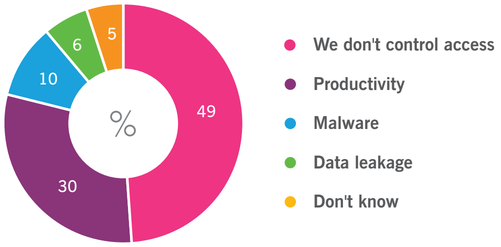
Network access control offers three main functions:

- » Authentication of users and devices, or verifying that they are who they say they are
- » Assessment of computers to check whether they meet your security criteria
- » Enforcement of policy, so that each user can access only information he or she is authorized for

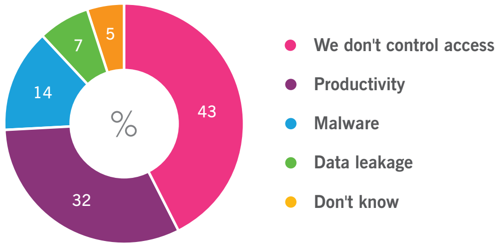
Although implementing NAC requires effort within your infrastructure (making sure routers and switches are enabled with the appropriate protocols), it is a worthwhile step when third parties, traveling users, telecommuters or contract workers need access to your network.

What is the primary reason for controlling access to*:

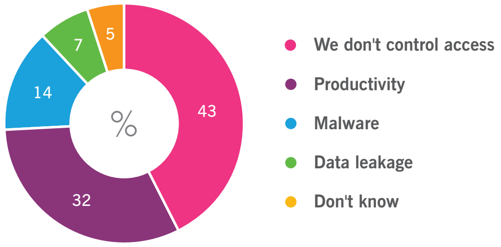
Twitter:



MySpace



FaceBook



*source: Sophos online poll December 2009

Network segmentation

Segmenting the network to keep unmanaged endpoints apart from your company's main network is a wise practice in security-sensitive settings, and for organizations that decide not to set up and maintain NAC. You can use a guest network to keep any unmanaged PCs within a quarantined zone. This separate network stops vulnerabilities or malware that are present on guest PCs from affecting other systems.

Physical or virtual segmentation using a VLAN is helpful when application control is impractical because users depend on software that is not issued by the company. For example, some organizations set up an engineering network so software testing does not affect other endpoints and users.

Patch management

Hackers actively seek to exploit vulnerabilities in browser, operating system and application software. Software vendors issue patches regularly for known security holes, and it is vital to stay up to date. Letting systems go unpatched is like leaving them open to malware and the damage it causes.

Application control

Application control allows you to block users from accessing applications that have security or productivity implications, including a category of applications referred to as potentially unwanted applications (PUAs). For example, some organizations control access to P2P clients, instant messaging or social networking sites.

The idea of application control is to decrease exposure to threats by limiting applications and restricting PUAs that are prone to malware. The more applications that you have installed, the more software patches you have to keep current with, so the risk of an unpatched vulnerability increases.

As noted earlier, strict application control isn't desirable when your users need specialized software beyond what your company usually supports. You can use NAC, network segmentation or both to increase security when application control is not a workable choice.

Device control

Uou reduce exposure to malware and data loss by controlling which devices, such as USB drives and smartphones, you let users connect to their PCs. Plugging in these devices or removable storage bypasses other layers of defense, which leaves you open to malicious executable files and data loss or theft.

Some companies establish a policy against connecting any device to better protect intellectual property (IP) and regulated data including personally identifiable information (PII). Other organizations enforce software scans before allowing devices to connect. Still others allow only company-issued devices, such as USB keys, to be plugged in.

Firewall

Today you are likely to use two types of firewalls. The first is a network, or gateway, firewall that surrounds your internal desktop systems and servers. The second is client firewall software that protects the endpoint PC on which it is installed. When a client firewall is location-aware, it enforces tighter controls depending on whether the user is connected to your trusted internal network or a non-trusted network, such as the Wi-Fi network at a coffee shop.

Anti-virus

Anti-virus software remains a core preventive mechanism against known viruses and other malware including Trojans, worms and spyware. Of course, you have to keep your anti-virus solution updated to counteract the latest threats. To stop unknown threats, the software also has to include proactive, behavior-based detection. Ideally these proactive measures should be integrated into a core agent, not separate components.

Encryption

Encryption protects your confidential information and enables you to comply with data security regulations, which may specifically require you to encrypt sensitive data. The information stored in an encrypted file or device can be accessed only with an encryption key or password.

Conclusion

No organization can afford to retreat from enabling its employees to do business online and take advantage of web-enabled technologies. Nor can you leave your systems and data exposed to malware attacks and intrusions. Closing security gaps with layers of protection that “interlock and block” not only from within the network but also at the endpoint offers effective protection that enables your business processes. Measuring each technology choice against the principles of prevention, proactiveness, performance and simplicity will help you avoid security breaches while ensuring your threat protection stays manageable and cost-effective.

To learn more about protecting your business from malware, visit www.sophos.com.

Sources

[1] http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=221901046

[2] http://www.networkworld.com/news/2010/012510-data-breach-costs.html

3. https://secure.sophos.com/security/whitepapers/sophos-bus-impact-of-data-security-regulations-wpus

4. http://www.sophos.com/security/topic/security-report-2010.html

5. http://www.sophos.com/security/topic/pci-compliance.html

6. http://www.sophos.com/security/topic/hipaa.html

7. http://www.sophos.com/security/topic/security-report-2010.html

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM