SOPHOS

Top 5 Threat Protection Best Practices

by **Chester Wisniewski**, Senior Security Analyst

Today's corporate networks face a barrage of threats, ranging from malware to accidental data loss. Your users' endpoints receive the brunt of these attacks, and if they are not properly protected they can serve as a threat portal to the entire network. The following top five best practices offer advice to help you protect your endpoints and your network against an ever-growing body of threats.

1 Control outbound content as well as inbound.

Data loss can be accidental or malicious. Human error, carelessness, or a lack of data security can lead to data loss, such as sending an e-mail attachment containing personally identifiable information (PII) to an unauthorized recipient. Most companies' firewalls are set up to block incoming traffic, but data is sent off network on common ports like IRC, SMTP, and HTTP.

Stop accidental data loss by scanning content for sensitive information sent by e-mail, instant message, or saved on storage devices with automatic rules. Set up a file matching rule that specifies an action to be taken based on the name or type of file a user is attempting to access or transfer, and a content rule that contains one or more data definitions and specifies the action taken if a user attempts to transfer data that matches those definitions. Upon detection you may wish to alert the user to the sensitive content and ask them for confirmation so they can decide if the action is appropriate.

» **For more information on controlling outbound content, download the Sophos white paper Protecting Personally Identifiable Information: What Data is at Risk and What You Can Do About It.**

2 To protect against malware, block access to Web ports and scan traffic.

With one new Web page infected every 4.5 seconds,* the Web is now the number one vector of attack for cybercriminals. Taking advantage of Web infrastructure vulnerabilities, attackers covertly inject malicious code into legitimate Web sites. This Web-based malware then uses social engineering tactics or browser vulnerabilities to infect visitors with the intention of stealing confidential data, installing more malicious code, or silently recruiting the host system into a botnet.

Use real-time predictive malware filtering technology to scan all Web traffic, and identify both known and emerging zero-day malware. Use content-based filtering technology to analyze Web traffic to determine the true filetype of content coming back from a Web site and allow or disallow the traffic based on corporate policy.

» **For more information on protecting your network against Web-based malware, download the Sophos white paper Enabling a Safer Internet: The Positive Approach to Web Security.**

** According to the Sophos Security Threat Report 2010*

3 Educate users about the dangers and safe use of social networking Web sites.

Social networking sites like Facebook and Twitter have become popular playgrounds for attackers who recognize users' tendency to instill a higher level of trust in the sites themselves and to share too much personal information. As a result, malware and data theft are presenting serious problems to their users. In fact, there was a 70% rise in proportion of firms that report encountering spam and malware attacks via social networks during 2009.* Spam is also common on social networking sites, and social engineering is on the rise.

Share this information with users and encourage them to use social networking sites with the same level of caution that they've learned to use when using other Web applications. If your business allows the use of social media sites consider drafting a policy on what information your users are allowed to share and how these tools should be used. They should also become familiar with and use the sites' privacy settings.

» **For more information on the dangers posed by social networking sites, download the Sophos Security Threat Report: 2010.**

4 Encrypt sensitive data in use, at rest, and in motion.

Encryption is an integral technology to protect your organization's sensitive data. If a threat bypasses your anti-virus, firewall, or other controls, PII (Personally Identifiable Information) is vulnerable. But if data that is encrypted before it's placed on removable media or sent by e-mail falls into the wrong hands, it is unreadable.

To ensure that data is always protected, it should be encrypted on end user devices (such as smartphones and laptops), when it is sent over the network, and when it is stored. You can provide the password or exchange keys to the encrypted data on a case-by-case basis among groups or individuals who require access to perform their jobs. Properly deployed encryption also provides a "safe harbor" from data breach disclosure regulations.

» **For more information on encrypting PII, download the Sophos white paper Protecting Personally Identifiable Information: What Data is at Risk and What You Can Do About It.**

5 Restrict use of removable storage devices.

An organization's vulnerabilities are exacerbated by the unchecked ability to launch unauthorized software from removable storage devices like USB keys, CDs, and DVDs. Unauthorized applications can introduce vulnerabilities to the network, and malware, like the Conficker worm, is becoming a major issue as these devices can serve as vehicles for distribution. Data can also be easily taken outside of an organization on these devices, and many recent high-profile incidents confirm how easily they can be lost.

Disable the auto-run functionality for these drives or remove them entirely from users' machines.

» **For more information on protecting your network against the threats posed by removable storage devices, download the Sophos white paper How to implement a data loss prevention strategy.**

To learn more about Sophos and to evaluate any of our products free for 30 days, please visit us at **www.sophos.com**

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM