



Securing the Network

Take precautions to keep your business network safe from threats.



Network security is a 24 hour a day, 7 day a week task. The Internet is a global entity, so it may be nighttime where you are, but the sun is shining somewhere on the planet. That means someone, somewhere is awake at any given moment trying to develop a new exploit or engineer a new attack that will take down your network or compromise your data.

While there are a multitude of threats that network administrators need to be concerned with, they aren't always the most noticeable. Some things, such as an e-mail inbox full of spam messages offering low mortgage rates, are much more apparent and seem to demand attention.

Acclaimed author Stephen Covey, in his best-selling book "The 7 Habits of Highly Effective People," illustrates that the tasks that seem most urgent and draw your attention are often not the tasks that are most important. There are truly important things, such as performing research for an important report that is due for your job or executing tasks assigned to you by your manager. The important tasks are frequently sidelined by busy work, which seems urgent but is not important. It is easy to get distracted by a ringing phone or incoming e-mail messages that hinder your ability to handle the truly important tasks.

Computer and network security operates in much the same manner. The issues that seem most urgent or that constantly demand attention are often mere nuisances and do not pose as serious of a risk to your network security as some less-obvious threats. While 100 spam e-mail messages may be very noticeable, simple e-mail messages do not pose any real threat to network security. However, if those spam e-mail messages contain a phishing attack aimed at luring users to a malicious Web site or a malicious file attachment that can infect the computer and spread throughout the network, then they warrant more attention.

Protecting the Perimeter

Traditionally, network security has taken an "us versus them" approach. The picture of network

security looked like a castle and moat, where anything in the castle is part of the internal network, the moat is the network perimeter, and anything outside of the moat is part of the insecure public network and may be a threat to the security of the internal network.

Network security relies on firewalls to act as the drawbridge over the moat. Simply put, the perimeter firewall is the gatekeeper to the internal network and represents the single point of access to get to the internal network.

To be effective, all incoming network traffic must pass through the firewall. The basic premise of protecting the network with a perimeter firewall is to block all incoming traffic unless there is a rule specifically allowing it. If there are Web servers on your network that the public should be able to view, a rule allowing traffic on TCP Port 80 (the default port for HTTP traffic) would be necessary. If there are e-mail servers on the internal network, a rule allowing traffic on Port 25 (SMTP) or 110 (POP3) would be necessary to allow the incoming e-mail to pass through.

The firewall treats responses to internal requests different than external traffic. So, blocking all incoming network traffic does not mean that users can't view Web sites. The Web data will enter the network as a response to a request from an internal computer to view that Web site. By blocking all traffic and then specifically defining rules for acceptable incoming traffic, you can limit the exposure of the network and provide a level of protection from outside threats.

Shrinking Borders

Firewalls on the network perimeter help to segregate the internal network from external traffic or attacks, but in many ways, the network perimeter no longer exists. With the advent of portable storage such as USB thumb drives or the ability to store data in portable MP3 players or in cell phones, threats that should be outside of the perimeter are often connected directly to the internal network. A more mobile workforce using notebooks at hotels and coffee shops means

devices that are technically part of the internal network are being used outside of the perimeter.

From a network security perspective, this means that each individual device or computer needs its own perimeter protection. Increasingly, small businesses are implementing security at the endpoint as well as the perimeter. The network firewall will still prevent unauthorized external traffic from entering the network, but a personal firewall running on the desktop computer or endpoint device will safeguard it from malware carried in on a USB thumb drive or from malicious attacks while using a notebook on a public wireless network.

Many of the security vendors, such as McAfee or Symantec, have recognized the shifting threat by moving from pure antivirus to security suites, which include personal firewall protection. Microsoft Windows comes with a built-in personal firewall as well. Many security experts feel that the Windows Firewall supplied by Microsoft is not as robust as its third-party competitors, but even just enabling this built-in firewall is better than providing no protection at all for mobile computing devices.

King of Your Own Castle

Having the network perimeter fade away has made protecting the endpoint computers that much more difficult. However, users logging in with accounts that have administrative access, or more rights and privileges than are actually necessary, also pose a problem.

In general, users want to have complete access to their computers. They generally prefer to be able to modify system settings, change desktop backgrounds, install new software and more. If users log in with standard user accounts, they are often unable to do any of these things. The trick is to find the right balance between functionality and security.

Designating administrator access to local users has implications on a number of levels. First, when users are able to install, uninstall and

reconfigure at will, maintaining the environment is much more difficult. It is virtually impossible to maintain a current inventory of what is installed in order to track vulnerabilities and deploy patches. If the standard build is monitored and maintained, there may still be programs and applications on the network with vulnerabilities that could allow an attacker access to network resources.

The other prevailing issue is that malware generally operates at the level of the current user. When a virus, Trojan horse or spyware infects a computer and attempts to execute files or propagate itself, it uses the rights and privileges of the user that is logged in. If the normal user is logged into the system with full local administrator access to the computer, the malware will have virtually unrestricted access to the computer and any connected network resources.

In general, user accounts with administrator rights should only be used when necessary — even by network and security administrators. For day-to-day use, users should be logged in with standard user accounts to limit the impact of malware and restrict the ability to change the system configuration.

Windows provides the “Run As” option to allow the use of different user credentials when necessary. By right-clicking on a file, such as a program installation executable, you can supply a different user name and password under which to run the program. Using this feature, it is possible to still be able to install software or perform tasks that require administrative rights without being logged in full time using an “Administrator” account and exposing the computer or network to unnecessary risks.

With Windows Vista, Microsoft altered “Run As” slightly to “Run As Administrator.” The net result is the same: It provides the ability to execute programs as an administrator without having to be logged in as an administrator all the time. It removes the ability to access or execute files using different, non-administrator credentials,

without having to log out and log back in using the other credentials.

Controlling Access to the Network

Regardless of where the network perimeter is located, organizations of all sizes need to be able to control access to network resources. The whole point of being able to define the network perimeter is to establish the border between internal or safe devices and resources, and external or potentially risky or vulnerable devices and resources.

The border is disappearing and it is difficult, if not impossible in some cases, to assume that any device is inherently safe or secure just because of where it sits in relation to the network perimeter. Users with notebook computers might use them from home one day, a coffee shop on the corner the next day and then sitting at a desk in the office the day after that.

You can't be sure what the notebook was exposed to or if it might have been infected or compromised while it was at home or at the coffee shop, so you can't assume it to be safe just because it connects from the internal network on the third day. Even for desktop machines or devices that are more permanently attached to the internal network, it is often difficult to control whether or not users have exposed them to any threats via portable storage such as USB thumb drives or MP3 players.

For some businesses, third-party devices are also a serious concern. Different business partners, suppliers, vendors or other users may visit for a few hours or a few days and need to access the network while they are there. In some cases, they may just want access to the Internet so they can get to their own internal company resources through a VPN or FTP site. If they are running a demo or pilot of some kind, they may need to be able to access or connect with internal network resources. Regardless of why they need access, allowing third-party devices onto your network is always a risk. With no control over their device configuration or basic security issues such as

patching and antivirus, you still need some level of assurance that allowing the third-party device to connect to your network will not adversely impact your overall network security.

One solution for allowing third-party access is to segment the network and provide them access to a network segment that is segregated from the rest of the network. Having vendors and suppliers connect to the network on a separate LAN or virtual LAN segment provides a layer of protection for the internal network.

A solution that encompasses internal devices, as well as third-party connections and rogue devices attached to the network, is NAC, or Network Access Control. A NAC solution inspects devices as they attempt to connect to the network and checks to ensure that the device meets specific standards before allowing it to connect.

There are various NAC solutions, such as the Cisco NAC appliance and framework. In a typical NAC installation, you can choose what to check for and define the minimum acceptable standard. The NAC will inspect devices attempting to connect to the network to determine things such as the existence and current level of antivirus, what patches are applied and other aspects of your computer security policy. Noncompliant devices can simply be denied access, or in some cases you can configure the NAC to redirect them to a site where they can review the organization's security policy and download any necessary applications or updates in order to properly secure their machine to access the network.

The Re-emergence of Spam

Spam has been the scourge of e-mail for a very long time. The sheer volume of unsolicited e-mail messages flying across the Internet and filling up inboxes has at times seemed to threaten the very efficacy of e-mail as a form of communication. It is difficult for users to be productive and take e-mail seriously as a method of communication if they have to filter through and delete 100 messages just to find one valid e-mail.

After having leveled and even slightly dropped by some estimates, the volume of spam, as a percentage of the total volume of e-mail messages, seems to be on the rise again. This is due in part to the use of e-mail spam to distribute malware such as Trojan horses and phishing attacks. But regardless of the reason, businesses need to have the right technology in place to ensure that spam e-mail does not impact their operations.

The common approach to the spam epidemic is to filter it at two levels. The first is to have some form of filter or e-mail gateway that examines all incoming messages and blocks or quarantines messages that appear to be spam. Using a spam-filtering appliance at the gateway can greatly reduce the amount of spam that is allowed into the internal network and reduce the impact the spam has on network bandwidth.

The second level of protection is on the e-mail client itself. Most e-mail clients now provide some type of spam-filtering capabilities; and many endpoint security suites include antispam along with antivirus, personal firewalls and other security tools. Providing some form of spam filtering at the desktop level increases the odds that a spam message will be identified and filtered before it gets to the user's inbox and impacts productivity.

Image Spam

Spam is a constant struggle for businesses. For every detection or filter that antispam vendors come up with, spam purveyors come up with a new delivery method. Recently, image spam has been a novel approach to circumvent spam filters. Because most spam filtering is based on evaluating the text of the message to determine its value, placing the text of the spam message into an image which is then embedded in the e-mail can trick many spam filters.

The delivery of image-based spam gets even trickier by using random pixel changes and minor modifications to the image to bypass

even those spam filters that are smart enough to analyze the image.

With e-mail newsletter spam, the spammers take a legitimate e-mail newsletter and insert their own image spam ad within the contents. The user is more likely to open the e-mail message because they subscribed to the e-mail newsletter. They expect it to contain legitimate information that they have requested to have delivered to their Inbox. The headers are forged to appear as if they are from the correct source, making it difficult for spam filters or the user to distinguish from legitimate e-mail messages.

From Nuisance to Malware

Spam itself is more of an annoyance than a threat. It takes up network bandwidth and has the potential to reduce productivity by stealing employee time in order to sift through unwanted e-mail solicitations, but it can't really do anything malicious to the network. It does, however, make for a very effective distribution method for malware and malicious code.

An unsolicited offer to refinance your home mortgage is just a nuisance. An unsolicited e-mail that asks you to open the "mortgage.exe" file attachment in order to calculate what your new mortgage could be is a threat to network security. The ability to attach files to an e-mail and instantly transmit data around the world is a tremendous convenience for businesses. But it is imperative that the users know what the file is and why it was sent to them before they open it. Otherwise, they may be triggering some sort of Trojan horse, virus or other malware.

Organizations need to control the types of files that are allowable in order to protect the network from naive users being lured into executing malicious programs that can endanger network security. E-mail gateways and servers generally offer some type of file attachment filtering. Blocking all file attachments would provide the greatest security but is not practical for a business. You need to identify the ways in which the business

uses e-mail and finds solutions that balance business needs with security concerns.

Typically, organizations identify the file types that are known to have been used to distribute malicious code — or file types that have the potential to distribute malicious code — and block those file types at the e-mail gateway. File types such as EXE, BAT and COM are all executable and could contain anything, regardless of the file name. These are almost universally blocked.

Shooting Phish in a Barrel

File attachments are not the only threat when it comes to spam e-mail messages. Some e-mail may not contain malicious code in the e-mail itself, but will attempt to lure unsuspecting users to visit malicious Web sites that may attempt to install malware on their system or try to trick the user into surrendering personal or confidential information such as passwords, credit card numbers or Social Security numbers.

These attacks are called phishing attacks because they attempt to use the e-mail as bait to lure unsuspecting users into voluntarily giving up sensitive information. The e-mail is often formatted and worded to appear as if it is from a retail chain or financial institution, and the link embedded in the e-mail typically leads to a Web site designed to look exactly like the actual Web site of the company being spoofed. If done properly, users are led to believe they are dealing with the institution being spoofed and will willingly supply the requested information.

While such attacks generate at least some success, broadcasting spam to such a large base puts a spotlight on the phishing attack and helps the spoofed vendor and security firms address the attack by having the phishing Web site blocked or taken offline faster. A stealthier form of phishing that seeks to fly under the radar by targeting a much smaller audience is spearphishing.

A spearphishing attack typically targets a specific company and attempts to gain user names and

passwords that will allow the attacker access to the network for future attacks. Rather than blanketing the entire Internet with e-mail, spearphishing attacks distribute spam e-mail only to addresses on the domain being targeted.

To defend against spearphishing, companies should have clearly defined policies about what information may be requested via e-mail and educate users not to share sensitive information, even with individuals claiming to be from the help desk or other company departments. Most spearphishing attacks can also be stopped by blocking e-mail coming in from the public Internet that claims to be from the internal domain.

Beware of Bots

Another security threat that seems to be nearing epidemic status is the spread of bots or botnets. In actuality, a bot is a legitimate tool created and used for the purpose of maintaining IRC (Internet Relay Chat) channels. The bot can be used to execute a variety of functions, which led malicious developers to hijack the concept to create a new breed of malware.

When a system is compromised by a malicious bot, the bot software installs itself, and the computer basically sits in standby mode waiting for commands from the botmaster or botherder. The botmaster typically has almost complete control of the compromised system. They can install and execute software, use the bot system to distribute spam e-mail messages, harness the bot system to perform a DoS (denial-of-service) attack against a specific Web site, and much more. These dormant systems are sometimes referred to as “zombies.”

From an enterprise network security standpoint, the concern extends to any sort of backdoor or keylogger components that might be a part of the bot or installed by the botmaster. Such tools may allow the attacker to capture sensitive information such as confidential corporate data, user credentials and more.

Bots are identified and blocked by the major antivirus software programs. The most effective defense to bots is to ensure that antivirus software is installed, up to date, and scanning in real time to detect and block threats. Another line of defense is to restrict outbound communications using a firewall to prevent computers on the internal network from opening ports and establishing communications with the bot network.

Evolving Role of Antivirus Software

It wasn't long ago that the various computer security threats were treated individually with point solutions. Viruses and worms were stopped with standalone antivirus software. Unauthorized traffic was stopped with a standalone firewall. Unsolicited e-mail messages were stopped by a standalone spam-filtering product. Spyware was detected and blocked by a standalone antispymware product.

Antivirus software has evolved over time to encompass all of the above. In fact, for most major antivirus products, the term antivirus is a misnomer. Many of the vendors have adopted the term "Security Suite" to identify the product as a collection of tools used in concert to detect and block threats. A more correct term for the state of antivirus today would be to call it antimalware, because the software is designed to detect and reject a wide variety of computer threats and not just viruses and worms.

Blended Threats

There are a few different reasons for the convergence of security software into suites or all-in-one antimalware products. One has to do with bang for the buck. Each of these security tools has become somewhat commoditized, meaning they all essentially do the same thing and there is often little that separates one product from the next. That brings the overall value down and makes users and companies less likely to invest significant amounts of money buying all of the various standalone solutions.

A bigger driver for the convergence of security software, however, has been the convergence of security threats. The threat landscape has evolved and matured. What used to be a virus created by a script-kiddie for a fleeting moment of fame and glory in the hacker underground has evolved into a full-blown business model being employed by organized crime groups with profit in mind.

Rather than just writing a virus, malware authors tend to incorporate aspects from across the board. This new breed of blended threat — a threat that combines facets from a variety of individual threat types — requires that the security software look at the whole picture. Running separate standalone products will provide protection, but not as efficiently or successfully as the combined antimalware product. A combined product will typically apply more intelligence in correlating events between the various security software components and will generally use fewer system resources because the redundancy of running separate scan engines can be reduced or eliminated.

Today, Unified Threat Management (UTM) firewalls add a range of security functions that have typically been available piecemeal as separate programs or devices, from virus protection to spam, phishing and spyware blockers. On the menu of UTM features, buyers can find intrusion prevention systems (IPS); content filtering functions; programs to block spam, spyware and phishing attempts; and even vulnerability scanning — software that probes for potential security gaps based on a network's defenses and known vulnerabilities. Yet every vendor offers a different mix of services in their UTM, and the mix can even vary within a single vendor's product line.

Spyware and Adware

Spyware has been called a number of things over the years. Initially, spyware was a term used for small programs placed on the computer that would track and log specifically targeted activities. That information was sent back to the spyware owner, who typically used it for

marketing purposes to better target products or services, or to refine and improve delivery of services.

Some companies were upfront about their motives and actions, and those applications were dubbed “adware.” Some companies installed their monitoring products without warning or acknowledgment, and those applications were dubbed spyware. Over time, those lines have blurred, and spyware overall has become much more malicious.

Attackers discovered that if a company could plant spyware to watch specifically targeted actions and report that activity back, then spyware could also be used to capture other information. Many spyware threats contain keystroke logging components to try to capture user names, passwords, credit card numbers, Social Security numbers and other sensitive information. In keeping with the blended-threat trend, spyware also often installs a backdoor component that might allow the attacker to remotely access the compromised system and execute other malicious programs on it.

Removing Spyware

Removing spyware is often tricky. Antispyware applications have improved and are much better today than in years past at detecting and blocking spyware threats, as well as identifying and removing them after the fact. Some threats are more tenacious than others though.

The majority of threats can be removed by updating the antispyware definitions of your security software and running a scan to detect and remove any identified threats. A handful of spyware threats embed themselves in memory and use registry hooks that make them exceptionally difficult to remove.

To remove troublesome spyware, you can try using a different antispyware product than you normally use. It may have more success against that specific threat. If that fails, you may need

to reboot your Windows machine into SafeMode to extricate the threat without allowing it to be loaded into memory. Or, you may need to use a tool such as HijackThis to monitor the processes on your computer and try to identify the specific processes associated with the threat so you can remove them manually.

Be Vigilant

Network security is obviously a big deal. Attackers continue to research and discover new holes to exploit and new attack vectors to employ, and you must remain vigilant to defend against these attacks. Not only is it important to ensure that your data and network resources are secure from a practical standpoint, but the regulatory environment today — including compliance issues with Sarbanes-Oxley, HIPAA, GLBA, PCI Data Security Standard and more — all mandate that you apply an appropriate level of security to safeguard your network.

It is important that you understand what the threats are and how to defend against them. But, it is equally or even more important that you understand your own network and implement security in a way that makes sense. Assess the roles of your equipment and define the critical components. Perform a risk assessment to determine which machines are more exposed than others and invest your security budget to maximize the effectiveness of your network security.

Stay informed about emerging trends, both in attacks and threats to your network security, and in the tools and techniques to protect your network. But, along with the knowledge of threats and protective measures, understand your business and the role your network plays in it. Ensure that your security measures help to facilitate and protect the business, and do not implement security just for the sake of implementing security. In most cases, budgets are tight. It is important that you invest the security budget in the most beneficial way possible. ■

