

How Internet Usage Puts Your Business at Risk

Introduction

Small and mid-size businesses have come to rely heavily on the Internet as an essential part of their day-to-day operations. It offers speedy access to information and enables 24x7 communications with the outside world. But despite the overwhelming benefits the Internet offers, it also inherently puts companies at risk from an array of security threats. Simply utilizing the Web puts the companies at risk of Internet-based threats that multiplies as online activity increases.

Inappropriate Usage

Companies that fail to filter or monitor their employees' Internet usage risk the productivity of their workforce, their reputation, and the security of their network. Employees can spend an exorbitant amount of time surfing the Web for both personal and business purposes. Many will visit online shopping, peer-to-peer, and social networking sites – even online dating or adult sites. All of these activities waste company time and expose the company network to Internet-based threats.

For example, adult sites are notorious for hosting malware. These sites are easy and inexpensive to launch, contain content that attracts numerous visitors, and are taboo enough to elicit silence from visitors who suspect they may have infected their system by visiting the site. These attributes make them the ideal medium for spreading malware.

Online shopping sites are equally as notable for hosting Internet-based threats as their adult site counterparts. Spyware runs rampant throughout many of these sites. Additionally, they frequently link to third-party sites for many of their items, completely transparent to the user. Therefore, even if the main site is trustworthy, the user rarely knows when he or she is on the "clean" site, or on one of an unknown third party.

In an annual survey on information security breaches, conducted by PricewaterhouseCoopers on behalf of the United Kingdom's Department of Business Enterprise & Regulatory Reform (BERR), it was discovered that as many as one in six businesses experienced staff misuse of their information systems in the past year. Of the cases reported, 36 percent were spending an excessive amount of time browsing the Internet, with an additional 41 percent accessing inappropriate Web sites. Though certainly less prevalent, employees accessing illegal content was also reported.

Much of this inappropriate usage, including questionable or risky behavior, can be attributed to the nonchalant attitude many employees have toward their employers' equipment. Many employees proceed throughout the Internet with the belief that since it is not their computer they are using, security is not important. Similarly, many users assume that security is the responsibility of IT, so risky behavior will not have any negative impact.

Vehicle for External Threats

Even when used appropriately by the company's employees, the Internet is the primary source for an array of computer threats, including spyware, Trojans, bots, backdoors, and rootkits. In many cases, the only user interaction required for an infection is to simply visit the site. This method of transmission, called a "drive-by download", occurs in the background during the normal course of the user's online activities – with neither the knowledge of, nor interaction from, the user.

Based on NETGEAR ProSecure research, 79 percent these threats have been discovered on legitimate sites which have been hijacked by hackers who have stealthily infected the site with the threat. In these attacks, hackers take advantage of Web vulnerabilities to insert threats on any site that has not yet applied the patch. As a result, any site can be affected. In the first quarter of 2008 alone, thousands of websites belonging to Fortune 500 companies, government agencies and schools reported being infected with malicious code. Even well-known security vendors such as Symantec, Trend Micro, and Computer Associates have had their Web sites compromised.

Attackers have also learned to use legitimate sites as bait for "social engineering" tactics, which attempt to trick users into clicking on an embedded link or on the email attachment. In December 2008, the popular social networking site "Facebook" was used in such an attack. An email arrived in users' inboxes with the subject line "You look funny in this new video". The email then encouraged users to use the embedded link to view the video. The link diverted to a video site not belonging to Facebook and informed the user that an update of the Flash player was necessary. Using the supplied link to take the recommended action installed a worm on the user's system. The worm included spyware and opened a backdoor which would enable private information to be sent from the system, as well as for additional code to be installed on it in the future.

The remaining 21 percent of these threats are the result of a user inadvertently visiting a rogue Web site. These sites are designed to appear legitimate, specifically to attract unsuspecting users. Many of them even utilize search engine marketing and banner advertisements to increase the number of visitors.

Drive-By Downloads

A drive-by download is a Web-hosted threat. It is a bit different than the previous threats mentioned, in that it relies on the victim coming to it, rather than being sent to the victim's system. In a drive-by download, threats such as spyware, adware, or trojans are installed with neither the knowledge of, nor any interaction by, the user. When the user visits an infected Web site, the threat is automatically downloaded in the background. The infected site can be a rogue site, developed by a malicious author to appear legitimate, or it can be a legitimate site that has been hijacked by the malicious author and subsequently infected with the threat. In either case, however, the user typically does not even realize an infection has occurred.

By implanting threats on legitimate sites, attackers gain a built-in audience. In developing their own rogue sites, they gain more control over the threat. In either case, it becomes apparent that blocking sites based on their content is no longer adequate to protect the company from such threats.

Protecting Your Business

The user's system is viewed by attackers as the path of least resistance to their real target — the company network. Therefore, many threats enter the network via the user's system, and then propagate freely. Once inside, these threats can consume significant amounts of network bandwidth, steal sensitive company and customer data, damage file systems, or hijack the company's assets for launching spam and other email-borne threats.

Therefore, the first line of defense against Internet-based threats is to establish and enforce an acceptable Internet use policy. The policy should clearly articulate the types of sites that are and are not permissible, as well as the amount of time deemed acceptable. However, most businesses allow some degree of personal Web activity using company equipment, and allowing employees too much freedom inherently puts the business at risk. The policy must not only cover the amount of time employees are allowed to spend on personal business on the Web, but also the type of sites they are allowed to visit.

In addition to usage policies, it is absolutely essential that the company install strong gateway security that includes URL, content filtering, and bi-directional traffic inspection. With URL and content filtering, the security appliance enforces company policies by blocking prohibited URLs and inappropriate content. When an employee attempts to visit either a specific site that has been banned, or one that contains content that has been prohibited by the company, the network transmission is blocked and a report is sent to IT.

It is important to remember that filtering only protects the company from a relatively small percentage of these threats. For more comprehensive protection, the appliance must also conduct real-time bi-directional traffic inspection to proactively protect against malware from sites that have not been specifically blocked. This adds a critical layer of defense to effectively protect the company against accidental infection via hacked legitimate Web sites, as well as rogue sites that have been crafted to appear legitimate. Traffic inspection monitors the inbound and outbound traffic every time an employee visits a URL. If an employee inadvertently lands on an infected site, the inbound traffic triggers the appliance, which immediately blocks the network transmission.

Conclusion

Any internet-connected company is faced with Web-based security threats, through the normal course of their daily activities. If the company lacks comprehensive gateway security, the risk becomes exponentially greater. The establishment and enforcement of acceptable usage policies, coupled with proactive real-time bi-directional traffic inspection will help mitigate this risk.

NETGEAR® ProSecure™ STM Web and Email Threat Management Appliance Solution

The ProSecure STM Appliance uses a unique technology that detects and blocks outbreaks based on their rapid and wide distribution behavior. This approach can detect spam and malware outbreaks as soon as they emerge, and block all associated messages in real time.

The ProSecure STM Appliance features patent pending Stream Scanning Technology that is designed to scan data streams as they enter the network. With Stream Scanning Technology, the NETGEAR STM is able to process large amounts of data in real-time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and Web content clean and without delay.

The ProSecure STM Appliance uses a proactive behavioral defense system that eliminates the gap between a vulnerability being exploited and the fix. The NETGEAR solution uses forensic analysis to identify suspicious characteristics of incoming and outgoing network traffic, and neutralizes them until they can be examined more closely.

NETGEAR, the NETGEAR logo, Connect with Innovation and ProSecure are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2009 NETGEAR, Inc. All rights reserved.