

# **Comprehensive Internet Security – Employing A Layered Defense**

## Introduction

Aircraft carriers employ a comprehensive layered defense strategy, beginning with proactive detection. Radar is utilized as the first line of defense, to detect any approaching attackers. When a threat is discovered, the aircraft carrier deploys the appropriate defense mechanism such as surface-to-air missiles or radar guided machine guns to protect the vessel from attacks. Each of these defenses play an overlapping role, yet they work together to ensure that the failure of any one of them does not lead to the demise of the vessel.

Similarly, IT managers must also deploy a comprehensive layered defense strategy. Rather than guns, missiles, and other weapons of traditional warfare, Internet based threats employ malicious software applications, known collectively as malware. Malware includes threats such as viruses, spyware, worms, trojans, backdoors, and keyloggers that propagate via email and Web. Over the past few years, blended threats, which are a combination of two or more types of malware, have become more prominent.

IT managers have long used anti-virus, anti-spyware, and other desktop-based security products to help protect against Internet-based threats. Though this may have once been adequate protection, the threat landscape has experienced extraordinary growth over the past several years. Security experts receiving approximately 500,000 unique malware samples in 2000 will receive an estimated 15 million by the end of 2008. New threat types and attack vectors are also continuously emerging. As a result, IT managers must develop comprehensive security measures which consider the wide array of threats. Much like the aircraft carrier, effectively averting these attacks requires a layered defense strategy.

## The Threat Landscape

As IT security professionals know, the threat landscape is continuously evolving. Malware has become more varied and increasingly complex. Early threats were confined to the desktop and were limited in scope and capabilities, while today's malware employ a multitude of techniques and vectors to attack on multiple levels – through email and Web to the company desktop and servers.

Early malware was limited to what could spread via floppy disks and other rudimentary vehicles, relying on users to spread it from one individual system to another. In contrast, modern-day threats employ a variety of propagation techniques, taking full advantage of the connectivity offered by the Internet. According to a recent Gartner study, the number of Web-hosted threats increased 800 percent in 2007<sup>1</sup>. Meanwhile, email is commonly used to direct users to the attack. Vulnerabilities in software applications, operating systems, and browser plug-ins offer attackers fast and efficient spreading capabilities. The common Internet connection also enables attackers to silently export credentials and other sensitive data from infected systems.

The other significant evolution in the threat landscape is the intent behind the threats. While past threats were traditionally developed by programmers seeking to impress their friends and fellow programmers, today's threats are largely propagated by criminals, seeking financial gain. These criminals are part of a growing \$100 billion underground market for computer threats. They consist of highly skilled malware authors who are hired to write the code that is required for the attack, organized crime groups and others who are intent on stealing sensitive personal information, and owners of email lists and other methods of propagation.

This continued proliferation of the criminal market puts unprotected businesses at more risk than ever before, with financially-motivated attacks threatening sensitive company and customer data.

## The Lack of Comprehensive Security

In a study conducted in June 2008, 81 percent of business computers lacked at least one essential security component, leaving the system vulnerable to attacks. The study assessed the security levels of 580 systems by looking at current patch levels, system-level firewalls, and client-side security software. 63 percent of the systems were missing at least one critical Microsoft security patch; 51 percent had firewalls that were disabled; and 15 percent had either disabled their security software, or had failed to keep it properly updated.

The problem does not exclusively reside with end users. Other studies have found similar results on the administrative end – with substandard levels of protection for email servers, Web servers, and application servers. The problem is particularly visible in small businesses that lack a full-time, dedicated IT department. Since many of these businesses do not possess the expertise on the various threats and the layers of security that are required to effectively combat them, the company can inadvertently leave itself exposed.

## A Delicate Balancing Act

Comprehensive security and usability are inherently at odds with one another. The most foolproof form of security would be to cut all communications with the outside world. Though certainly secure, that would not be a very practical solution. Likewise, allowing all inbound and outbound traffic with no regulation whatsoever would certainly enable employees all the freedom they need, but would open up the organization to attacks. Therefore, the approach must strike a balance between security and usability.

<sup>1</sup> Gartner research document #158459, "Why Malware Filtering Is Necessary in the Web Gateway", August 26, 2008.

## Going Beyond the Desktop

Ensuring that the organization is safe from Internet-based threats, while retaining the level of communications employees need, requires a more comprehensive approach to the problem. With a layered security model, the IT staff first assesses potential points of entry, then implements a security solution specifically to secure that point.

End-user security software, though certainly an important first step, is not sufficient to keep the company's network assets safe. This is true for two overarching reasons:

1. **End-User Systems Cannot Be Adequately Controlled.** As mentioned in the study above, end users often disable their security software, or fail to update it regularly. Though a hands-on IT department can push security updates manually, the growing trend toward a mobile workforce significantly undermines the effectiveness of this solution, since policies can only be pushed to systems when they are connected to the network. If a laptop is infected while disconnected from the company network, the infection can spread throughout the organization once that client is re-connected, long before IT can push any updates.
2. **The Internet Gateway Is the Primary Entry Point.** When the end user is connected to the company network, Web and email threats must first pass through the organization's Internet gateway, prior to reaching the end user's system. Blocking such threats at the Internet gateway is therefore more proactive and efficient. This also provides IT with a greater degree of control, since they manage these assets themselves, rather than having to rely on end users.

With these points in mind, it is essential that organizations secure their Internet gateway, to provide adequate protection from Internet-based threats.

## Email Inspection

Email remains a popular vector for a wide range of threats. Spam, phishing attacks, and malicious attachments are all common methods employed to introduce threats into the business environment. Additionally, infected end-user systems can be used to send inordinate amounts of spam, unbeknownst to the user. Therefore, it is important to inspect and filter both inbound and outbound email traffic at the gateway.

Inbound email inspection can help the organization proactively thwart a wide range of email-borne threats, including spam, viruses, spyware, phishing attacks, and inappropriate content. This is critical, since it provides a vital line of defense to ensure the threat never touches end users.

Outbound email inspection, though often overlooked by organizations, is another essential component to the business's layered security strategy, since it may provide the only indication of an infection within the organization.

## Web Protection

World Wide Web usage has become part of our everyday lives and, indeed, there are many legitimate business uses for the Web. However, the Web also provides a fertile vehicle for malware and other Web-based attacks. 79 percent of all Web-based threats have been found on legitimate sites that have been hijacked by attackers and subsequently infused with malicious applications. Additionally, inappropriate sites often contain spyware, and rogue sites can appear legitimate and gain a significant number of visitors through online searches, phishing attacks, and other methods.

To enable legitimate Internet use while maintaining proper company security requires a healthy degree of scanning for viruses and other malware, as well as URL filtering. As with email, scanning both inbound and outbound traffic is key. Inbound scanning determines if any Web traffic is attempting to deliver malware, if a malicious program is attempting to download, or if a user is downloading malware by accident. Outbound scanning adds another layer of defense by detecting if a spyware program attempts to "phone home", sending sensitive data to the malicious author that it has collected from the user's system.

## Conclusion

Internet-based threats are a prominent and growing component of the overall threat landscape. These threats can take a variety of forms and utilize any number of propagation techniques, thereby rendering desktop-based security by itself to be an inadequate defense mechanism. Instead, IT managers must develop more comprehensive security policies to protect against them. Taking a layered defense approach, supplementing desktop security with inbound and outbound inspection of both Web and email traffic, IT managers can effectively protect the company against the dangers of Internet attacks.

---

## **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.