Realtime publishers

How to Protect Your Business from Malware, Phishing, and Cybercrime

The SMB Security Series

Streamlining Web and Email Security

sponsored by

McAfee®

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Streamlining Web and Email Security

The Web and email systems are digital gateways into your business. Your customers and business partners can make use of your Web applications to conduct business with you and many depend on email for communications. These are valuable assets to any business, but they are also the means by which attackers can gain access to your systems and your confidential information. In today's business environment, it is imperative that you protect your Web-based assets and secure your email systems to mitigate the risk from well-known threats such as malware, spam, phishing, and data loss.

This final article in the *SMB Security Series: How to Protect Your Business from Malware, Phishing, and Cybercrime* describes threats to your systems and provides guidelines for protecting those systems. In particular, we will examine:

- Malware and attacks entering your system
- Protecting network traffic
- Resources for addressing security risks
- An executive checklist for evaluating options

These topics reflect the multiple dimensions of security threats and the combination of measures that must be in place to mitigate the risk posed by these threats.

Malware Attacks Entering Your Environment

Malware and other forms of attacks can be categorized by the type of application exploited, including email systems, Web browsers, and other applications. We have discussed email-based threats including malware and phishing lures. Malware comes in many forms and attackers have used email as a means of transmitting their code. As improvements in malware detection and advances in operating system (OS) security make it more difficult to deliver and activate malicious programs, attackers are turning to luring victims into infecting their own machines.

Phishing lures are crafted to appear like legitimate messages, for example, an email message may contain an attachment labeled "Recruitment Plan Q3.xls" along with a brief message asking for review comments. The spreadsheet may contain malicious code that exploits a vulnerability in another application and ultimately results in additional malicious code being installed on the compromised machine.

In addition to phishing lures that carry malicious code directly, some lures direct their victims to malicious sites. Once on those sites, attackers can use cross-site scripting attacks and exploit browser vulnerabilities to download malicious content.

Our own enterprise applications can be used against us as well. Poor input validation, SQL injection attacks, and other forms of injection attacks can be used to make applications perform operations they were not intended to perform. For example, an attacker may take advantage of poor input validation to craft a malicious SQL query on a database. Poorly written programs may simply assume that all input from a user is valid and run it without basic checks. This type of vulnerability is the basis for the success of injection attacks in which malicious code is injected into an application.

Anti-malware can help protect your business against malicious software delivered using email or the Web. Injection attacks and related application vulnerabilities can be detected using code reviews and vulnerability scanners. In addition, network traffic can be analyzed and filtered to further mitigate the risk of such attacks.

Protecting Network Traffic

A multi-tier approach is needed to protect network traffic and begins with defining security policies. Policies define expectations for IT professionals and end users with regards to protecting information assets. For IT professionals, polices define what kinds of security controls should be used, such as anti-malware, firewalls, access controls, and so on. Policies also define how these controls should be deployed and configured; for example, all endpoints should have anti-malware and firewalls deployed. Policies should take into account the varying requirements of different types of endpoints. For example, all endpoints may have the same configuration for anti-malware but servers should have firewalls configured according to the applications run on the server and services provided.

All traffic, both incoming and outgoing, should be scanned for malware, spam, and phishing lures. Scanning traffic should not adversely affect other services, such as timely email delivery, so be sure to size servers and other devices running security software to maintain adequate throughput.

Cybercrime is a global threat, and companies exist today that offer monitoring services and collect intelligence on cybercrime activities. For example, monitoring companies may be able to detect command and control nodes in spam-generating botnets. Information about these servers can be used to shut them down or protect your network from traffic originating with these servers.

The combination of anti-malware, anti-spam, anti-phishing, and firewalls along with monitoring and intelligence gathering services can reduce the chances that malicious software or lures will make it to an end user. This is important because we humans can be the weakest link in a security system. As victims of phishing scams can tell us, well-crafted emails or Web sites can lure us to click a link or open a file without much thought.

Resources for Addressing Security Risks

Your IT staff is your primary resource for addressing security risks. Small and midsize businesses often do not have the ability to have dedicated security staff specializing in different threats. It would not be unusual for the person responsible for managing Microsoft Exchange Servers to be the key person in charge of securing email against malware and spam. Similarly, the systems administrator responsible for servers hosting company Web sites and Web applications may also be the go-to person for application security. In such cases, it can be advantageous, and cost effective, to bring in outside contractors or consultants for short periods of time to make assessments, recommend security control options, and help implement them.

We should keep in mind the existing demands on IT staff. There may be room to place additional responsibilities for security on your staff, in which case you may want to have a completely in-house security solution. If your IT staff is already at maximum capacity workload, then security as a service may be a more appropriate option.

Executive Checklist for Evaluating Options

Executives will have to make choices about how to deploy resources and allocate funds for information security for Web and email services. When doing so, remember to keep in mind the risks and threats to information systems because each of these risks should be addressed. These risks include:

- Malicious software
- Spam
- Phishing attacks
- Data loss
- Loss of control of computing devices, for example due to a botnet infection

The options for responding to these threats include:

- Defining policies and procedures specifying how the company will address specific threats
- Implementing security controls, such as anti-malware, anti-spam, anti-phishing, firewalls, and data encryption
- Implementing management practices, such as reviewing logs and generating alerts to notify systems administrators when adverse events occur
- Subscribing to global monitoring services that provide additional protections not available to in-house solutions, such as blacklisting known malicious sites

The key decision-making criteria associated with this checklist are cost and effectiveness. We cannot eliminate risks and we can only mitigate risks to the point where the benefits outweigh the costs. To get the greatest benefit from our security resources, we should prioritize security needs. Some resources are more likely targets than others. If you have an application that stores financial information about customers, it should receive substantial attention with regards to formulating appropriate security measures. Employee-owned devices, such as smart phones, should also be controlled. The devices themselves may be owned by an employee, but they may access highly-valued corporate information. Access from remote consumer devices should also be considered a high-priority area.

Summary

Small and midsize businesses are not immune to information security risks. Malware, spam, and phishing scams can lead to data breaches, financial losses, and compromised computing and network resources. Security software and practices have advanced to the point where you do not need to have a group of in-house security experts to protect your systems. With the right security software and proper policies and procedures, small and midsize businesses can realize substantial security benefits. Improvements in delivering security as a service is opening a new option for companies looking to improve their information security without bring additional systems in-house.