Realtime
publishers

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

The SMB Security Series

Securing Endpoints without a Security Expert

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

Securing Endpoints Without a Security Expert

Businesses have to protect their endpoint devices from a wide range of security threats. Fortunately, we do not have to be specialized security experts to get the job done if we understand some of the fundamental issues of securing our business systems. In this, the second article in the *SMB Security Series: How to Protect Your Business from Malware, Phishing, and Cybercrime,* we examine how to implement and maintain endpoint security with particular emphasis on:

- The changing landscape of endpoint devices
- Core requirements for endpoint security
- Management requirements for maintaining endpoint security

By considering both the technical and management issues related to endpoint security, we can better understand how to mitigate the information security risks facing most businesses.

Changing Landscape of Endpoint Devices

When business information technology began decades ago, IT professionals worked with single, monolithic mainframe computers, dedicated terminals for interacting with the computer, and centralized storage systems dedicated to the needs of one system. Today's IT environment is radically different.

A typical IT department in today's business is responsible for managing a highly-distributed set of computers, network devices, and storage arrays. There are different types of devices ranging from small handhelds to large clusters of servers. In spite of the many differences in these devices, there is a common need for security controls on all of them.

An inventory of the various types of devices found in today's businesses includes:

- Desktop computers, which are typically used by a single individual and directly connected to a company's network.
- Laptop computers, which again are typically used by a single individual but are sometimes directly connected to the company network and are other times used remotely.

- Mobile devices, such as smart phones and tablet devices, which provide constant remote access to business services, such as email and calendar applications.
- Servers are often housed in a data center and provide shared services to the company, including email, Web hosting, file sharing, databases, and other enterprise applications.
- Newly instrumented devices, such as point of sale terminals, specialized medical devices, automobiles, and other devices that can collect data from multiple places and send it to centralized servers for analysis and storage.

Despite the differences in these device types, they can all function together on an integrated network (see Figure 1).

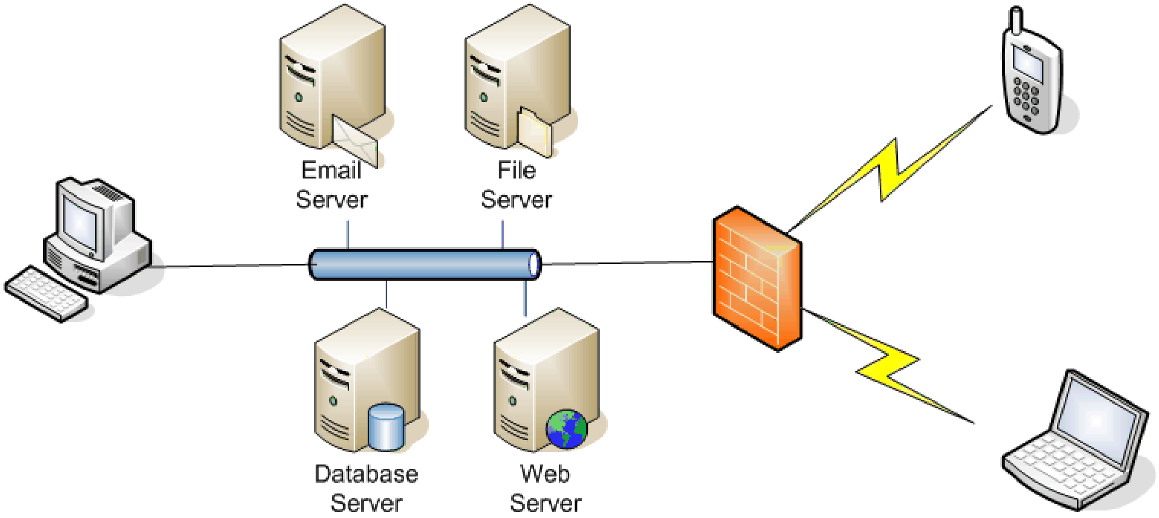

Figure 1: Endpoints vary in function and characteristics, but they all function together on a company's network and require similar types of endpoint security controls.

In addition to the diversity in device types, IT professionals are faced with the increasing use of personally-owned devices. It was not uncommon several years ago for employees to work from home using a home computer, but the level of use of personal devices has increased significantly with the availability of low-cost mobile devices such as smart phones and tablet devices. The addition of consumer devices makes management more difficult. It is important to have policies in place that describe acceptable use of personal devices and define what security measures must be taken before a personal device is used to access company resources.

These policies should describe:

- Required antivirus software
- Limits on the kinds of operations that can be performed while connected to the corporate network
- Limits on the types of information that can be permanently stored or cached on a personal device

Regardless of whether a device is a company asset or a personal device, all endpoints should be protected with a core set of security controls.

Core Requirements for Endpoint Security

Endpoints should be protected by several types of security controls:

- Anti-malware
- Anti-spam
- Anti-phishing
- Firewall
- Endpoint encryption

Anti-malware programs should be installed on endpoints to detect, contain, and remove malicious software. This type of software has long been called antivirus but that name does not reflect the full range of malicious code these programs can detect. Anti-malware should be configured to scan incoming content, such as downloaded attachments, as well as data on storage devices on a regular basis.

Anti-spam software is essential to keep unwanted email from clogging users' inboxes, consuming storage, and wasting network bandwidth. To get a sense of just how bad the problem is, consider these statistics (Source: Email Statistics Report 2010. The Radicati Group, Inc.):

- In the US, approximately 73% of all email messages are spam
- A midsize company of 1000 can spend approximately $3 million per year to deal with spam
- 1 message out of every 169 contains some type of malicious content
- 1 message out of every 242 is a phishing lure

Anti-phishing software is similar to anti-spam and anti-malware scanners in that it examines incoming traffic. Phishing lures sometimes contain links to malicious Web sites, so scanning messages for potentially harmful links is an important element of anti-phishing controls.

Firewalls are designed as gatekeepers to control the type of network traffic entering and leaving a device. Clearly, we need blocks on unwanted incoming traffic. Firewalls can be configured to block ports that are not needed. For example, most devices may block traffic on port 21, which is used, by convention, for ftp file transfers. Unless the device will use ftp, it is best to block traffic on that port to mitigate the risk of an attacker exploiting a weakness in ftp.

Outgoing traffic should also be controlled with firewalls. In particular, we should not assume that any traffic originating from one of our devices is trusted traffic. If an attacker were able to infect a computer with malicious software, that software may attempt to send information from the compromised device to an attacker-controlled server.

Valuable intellectual property or confidential information may reside on a number of devices in your business. These are all potential targets for a data breach. One way to mitigate the risk of data loss is to use endpoint encryption. With endpoint encryption, as long as an attacker does not have the decryption key, the information on the device is inaccessible.

The combination of anti-malware, anti-spam, anti-phishing, firewalls, and endpoint encryption create a multi-layered set of defenses that complement each other. If an attacker is able to circumvent anti-phishing measures and lure a victim into downloading malicious content, the anti-malware software can detect it. If someone is able to install a remote control program, the firewall may block its communications with a command and control server. If a thief were able to steal a laptop, the confidential information on the device could be protected by encryption. In addition to these technical requirements, there are management issues one should consider for complete security.

Management Requirements

Security software should be deployed on all endpoint devices, so ease of installation and maintenance is a key requirement. Once the software is installed, it should be configured to automatically update. As noted in the first article in this series, anti-malware vendors are detecting tens of thousands of new forms of malware every day. Trying to keep all endpoint devices up to date manually would be a poor use of staff time and would likely lead to mistakes that leave devices more vulnerable than they otherwise would be.

Anti-malware and other endpoint security controls should be configured to generate alerts for users and systems administrators when specific types of events occur, such as malicious content is found in an email message. These applications should also keep a log of significant events. This can be valuable information for analyzing a security breach as well as understanding overall trends and patterns affecting endpoint devices—assuming proper security management reporting is in place.

Anti-malware programs should support on-demand scanning and should work with removable as well as fixed storage devices.

A common management consideration is cost. There may be cost advantages to procuring suites of security software that include anti-malware, anti-spam, anti-phishing, firewalls, and endpoint encryption in a single package. These controls may also be available through security as a service from vendors. This delivery mechanism avoids the need to install and maintain security software on site.

Summary

Endpoints of all types must be protected against common malware, phishing, and data loss threats. When evaluating solutions, be sure to consider options with a comprehensive set of security controls and consider security as a service options as well. Also keep in mind the management requirements as well as technical requirements when assessing the best way to protect your business from malware, spam, phishing, and data loss.