

## Introduction

Computer security was once thought to be the exclusive province of somber men in dark suits and nerdy, whey-faced hackers. While both of these archetypes are still well-represented in the computing industry, the last two years have witnessed an explosive growth in the number of organizations that are seeking to boost the strength of their security. I attribute this growth to a number of factors:

- Increased public awareness of security and privacy problems on the Internet and in private networks. While most of the media attention has focused (unfairly) on Microsoft-specific problems, the sad truth is that the Internet infrastructure we depend on daily is riddled with holes, as are commercial operating systems of all stripes—not just Windows.
- Expanding value of information assets. For many businesses, the entire value of their operations is tied up in bits sitting on disks; software firms, financial traders, and other non-manufacturing businesses often don't have any physical inventory or assets, apart from office furniture and the like.
- Growing awareness of the legal and financial liability associated with security breaches. Various organizations, including the FBI, the General Accounting Office, and assorted security firms, have produced estimates for the yearly toll of computer crime that range from “we don't know because most places don't report intrusions” to laughably high multi-trillion dollar amounts. However bogus they appear, these estimates have laudably helped focus attention on the fact that when your network is attacked, there is a real cost—someone has to repair the compromised machines, restore their data, and so forth.

Because of these factors, more and more organizations want to improve their network and operational security. This book is intended to help you assess the security of your Exchange 2000 messaging systems, and then fix any deficiencies you find.

---

### Who This Book Is For

This book is written for Windows administrators with some Exchange 2000 experience. Throughout the book, I assume that you're familiar with basic Exchange 2000 concepts like storage groups and connectors, and that you have a passing understanding of Active Directory in particular and Windows 2000 in general. However, I realize that many potential readers are security analysts or administrators who are looking for guidance on securing what may be an unfamiliar system. Accordingly, the end of each chapter includes a list of recommended readings that will help fill in any gaps in your education.



Chapter 9 discusses one area where Exchange is fairly weak: content filtering and scanning. Don't despair, because part of this chapter is dedicated to evaluation criteria you can use when choosing a third-party content filtering product.

Chapter 10 is all about viruses; more specifically, it's all about how to keep them out of your Exchange system by providing multiple layers of defense.

### **Part III: Communications Security**

Once the underlying server is secure, you're ready to start worrying about the security of its communications channels.

Chapter 11 delves into the requirements for protecting your server's communications with TLS and IPsec, as well as how to use Microsoft's Internet Security and Acceleration (ISA) Server to securely publish Exchange services for MAPI clients.

Chapter 12 is dedicated to public-key infrastructure material, including explanations of how to set up your own PKI and what you can do with it. This is a fairly deep topic, but the information here will help you understand how to deploy an Exchange-ready PKI.

### **Part IV: Client Security**

When most people think of messaging security, they're really thinking about client security—specifically, Outlook security. However, there's more to it than that.

Chapter 13 is indeed dedicated to Outlook security, ranging from a discussion of attachment security management to a discussion of how to use its built-in S/MIME features.

Chapter 14 discusses the fascinating and complicated topic of securing Outlook Web Access; this was probably my favorite chapter to write, because I learned a great deal while researching it. Many users never run anything with "Outlook" in its name; they're using POP3 or IMAP4 clients like Netscape Communicator, Evolution, or Eudora.

Chapter 15 describes how to secure your server so that Internet-protocol clients can safely use it.

### **Part V: Advanced Topics**

Every book has some material that doesn't fit into its structure; in this book's case, there were two chapters that cried out to be included but didn't really belong elsewhere in the book.

Chapter 16 covers security for Exchange's Instant Messaging service, which is increasing cha 0 TDo4y05 Tc77-0.0178 -23.19g ab-0.t 8 066 Tf0.2216 0 TD0.0008 Tc0.0286 Tw(s ca TD3ueasin)9



---

## Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at <http://microsoft.com/mspress/support>.

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal Mail:

*Microsoft Press*

*Attn: Editor, Secure Messaging with Microsoft Exchange 2000*

*One Microsoft Way*

*Redmond, WA 98052-6399*

E-mail:

*[tkinput@microsoft.com](mailto:tkinput@microsoft.com)*

Please note that product support is not offered through the mail addresses. For support information, visit the Microsoft Web site at <http://www.microsoft.com/support>.



