

ion

thought to be the exclusive province of somber men
-faced hackers. Although both of these archetypes are
omputing industry, the last two years have witnessed
umber of organizations that are seeking to boost the
ribute this growth to a number of factors:

is of security and privacy problems on the Internet
Although most of the media attention has focused
ecific problems, the sad truth is that the Internet
on daily is riddled with holes, as are commercial
ipes—not just Microsoft Windows.

ation assets. For many businesses, the entire value
ip in bits sitting on disks; software firms, financial
ufacturing businesses often don't have any physi-
rt from office furniture and the like.

What's in This Book

This book is divided into five parts, each of which focuses on a particular set of topics.

Part I: Security Fundamentals

Chapter 1 is a gentle introduction to security concepts and buzzwords. It's designed to indoctrinate you to the way security professionals think about security, beginning with establishing a common vocabulary and set of concepts.

Chapter 2 focuses on security algorithms and protocols, including those used to provide encryption, authentication, and message integrity. Although this chapter features lots of acronyms, the topics discussed here are useful because they form the backbone of all of Exchange's security features.

Chapter 3 examines the security features of Windows. These features are important because Exchange depends on them; although there are a few Exchange-specific security features, most of what we think of as Exchange security is actually provided by the underlying operating system.

Chapter 4 is a survey of risk assessment. Entire books have been written on this topic, and there are trained professionals who can help you precisely quantify what risks your organization faces. This chapter gives you a head start on figuring out what you really stand to lose if you suffer a successful attack.

Chapter 5 covers operational security, the discipline of not revealing information about your environment unnecessarily. "Loose lips sink ships" is still the watchword, and this chapter helps point out some ways that you might unknowingly be leaking information.

Part II: Exchange Server Security

This part discusses, in depth, how to secure your Exchange server by hardening the underlying Windows configuration, installing Exchange securely, and protecting yourself against viruses, spam, and "bad" content.

Chapter 6 is devoted to Windows hardening. Even if you think you're in good shape, you should read it carefully and make sure that your patch evaluation and distribution system is set up properly.

Chapter 7 covers the intricacies of installing Exchange securely: giving the right permissions to the right people. Even though you've probably already installed Exchange, this chapter is worth reviewing to ensure that your permissions accurately reflect what you want people to be able to do.

Chapter 8 describes how to control Simple Mail Transfer Protocol (SMTP) relaying and spam. Exchange Server 2003 ships with good defaults for this already, but you should definitely understand what these settings do, when to change them, and when to leave them alone.

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 Transport Layer Security (TLS) and Internet Protocol Security (IPSec), as well as how to use the Microsoft Internet Security and Acceleration (ISA) Server to securely publish Exchange services for Messaging Application Programming Interface (MAPI) clients.

Chapter 12 is dedicated to public-key infrastructure (PKI) 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 helps 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, Microsoft 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 Secure Multipurpose Internet Mail Extensions (S/MIME) features.

Chapter 14 discusses the fascinating and complicated topic of securing Microsoft Outlook Web Access and front-end servers. Many users never run anything with "Outlook" in its name; they'

Chapter 17 describes how to comply with discovery, archival, and retention requirements. These are particularly important if you're in an industry like finance or health care, but every administrator should understand the basics in case of legal necessity.

Chapter 18 discusses security auditing and logging, including tips on suspicious event patterns or clusters you should be looking for.

Chapter 19 presents a security checklist that you can use to begin assessing the status of Exchange servers you're responsible for.

Chapter 20 outlines the legal concerns and issues surrounding messaging. It's not legal advice, but I can almost guarantee you'll learn something unexpected from it—the actual law, and administrators' perceptions of it, can vary quite a bit.

Appendices

Appendix A reprints two classic essays from the Microsoft Security Response Center: The Ten Immutable Laws of Security and The Ten Immutable Laws of Security Administration. Although these aren't printed on stone tablets, they remain valuable reading.

Appendix B is a detailed guide to the permissions applied at installation time.

What's Not in This Book

There's a great deal I had to leave out; after all, this book is about securing Exchange messaging systems, not a general treatise on securing Windows. Even within Exchange, I had to choose what could fit in the time and space allotted for the book. Accordingly, there's no coverage of security for real-time conferencing or migration security. Even though some sites will still be using the Exchange 2000 Server instant messaging service, or the Exchange 5.5 or Exchange 2000 Server chat services, in conjunction with Exchange Server 2003, those topics aren't covered either.

Conventions Used in This Book

Throughout this book you will find special sections set apart from the main text. These sections, denoted by icons, draw your attention to topics of special interest and importance or problems implementers invariably face during the course of a deployment. These features include the following:



Note This is used to underscore the importance of a specific concept or to highlight a special case that might apply only to certain situations.

More Info When additional material is available on a subject, whether in other sections in the book or from outside sources such as Web sites or white papers, such information is called out with the More Info icon.



Caution The *I told you so* of book features. When failure to take or avoid a certain action or situation could spell trouble for you, I point this out with the Caution feature.

Tip This feature is reserved for directing your attention to advice on time-saving or strategic moves.

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://www.microsoft.com/learning/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 Server 2003
One Microsoft Way
Redmond, WA 98052-6399*

E-mail:

mspinput@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>.

