

Securing Windows 2000 Server Documentation

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-02/0052.html>

From: Michael Howard (mikehow@MICROSOFT.COM)

Date: 02/25/03

Date: Tue, 25 Feb 2003 14:20:12 -0800

From: Michael Howard <mikehow@MICROSOFT.COM>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

The Microsoft Solutions for Security team has released 'Securing Windows 2000 Server'. This is the first of several prescriptive security solutions planned for release this year. These new security solutions are designed to provide customers with authoritative, proven, and tested solutions that address today's security challenges and business requirements.

The contents include:

Chapter 1: Introduction to Securing Windows 2000 Server This chapter introduces the Securing Windows 2000 Server guide. It includes a brief overview of each of the other chapters.

Chapter 2: Defining the Security Landscape This chapter focuses on defining security components that need to be understood to perform a security analysis of your organization. General guidance on how to perform a preliminary asset analysis for your organization is offered. The relationship between threats, exposures, vulnerabilities, and countermeasures is also explained.

Chapter 3: Understanding the Security Risk Management Discipline Proven practices are drawn upon in this chapter, from security analysis methodologies in use today that leverage the MSF and MOF. The SRMD also is defined in detail in this chapter, which provides learning that can be applied to assess and determine the level of risk in your own environment.

Chapter 4: Applying the Security Risk Management Discipline The SRMD is put into practice throughout this chapter to determine which threats and vulnerabilities have the most potential impact on a particular organization. This chapter applies this process to a generic scenario in which a fictitious company is used to illustrate how a set of common implementation decisions, and, therefore, a significant number of real-world vulnerabilities, should be determined. At the conclusion of this chapter, the specific risks addressed are fully defined, described, and analyzed.

Chapter 5: Securing the Domain Infrastructure Determining the criteria on which to base decisions that impact the organization at a domain level is the focus of this chapter. A high level overview of the Microsoft(r) Active Directory(r) service design, the organizational unit (OU) design, and domain policy is provided. In addition, specific domain policies that are implemented at Contoso, the fictional customer scenario used in this guide, are discussed in detail.

Chapter 6: Hardening the Base Windows 2000 Server The base settings applied to the member servers at Contoso are explained in this chapter. Group Policy was used to apply as many of the changes to the default Windows 2000 Server configuration as possible. For the member servers in this scenario, the Group Policy settings described are stored in the security template, MSS Baseline.inf. This template was imported into the Member Server Baseline Policy group policy, which is linked to the Member Server OU.

Chapter 7: Hardening Specific Server Roles The domain controllers, file servers, network infrastructure servers, and Web servers in any organization require different settings to maximize their security. This chapter focuses on the domain controllers and the other primary member server roles to show the steps that you should take to ensure that each of these roles is as secure as possible.

Chapter 8: Patch Management

This chapter shows how to ensure that an environment is kept up to date with all the necessary security patches; how to find out about new patches in a timely manner, how to implement them quickly and reliably, and how to monitor to ensure that they are deployed consistently.

Chapter 9: Auditing and Intrusion Detection This chapter shows how to audit an environment to provide the best chances of spotting attacks. It also looks at intrusion detection systems – software that is specifically designed to detect behavior that indicates an attack is occurring.

Chapter 10: Responding to Incidents

This chapter covers the best ways to respond to different types of attack and includes the steps that you should take to report the incidents effectively. It also includes a case study to illustrate a typical response to an incident.

Chapter 11: Conclusion

This chapter closes out the solution guide by providing a brief overview of everything that has been discussed.

The guides are available at:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/SecWin2k/Default.asp>

NT-Bugtraq: Securing Windows 2000 Server Documentation

PDF versions of the guides as well as the scripts, security templates, and job aids can be downloaded at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9964cf42-e236-4d73-aef4-7b4fdc0a25f6&DisplayLang=en>

Cheers, Michael
Secure Windows Initiative
Writing Secure Code 2nd Edition
<http://www.microsoft.com/mspress/books/5957.asp>

oo
Delivery co-sponsored by TruSecure Corporation
oo
TICSA – Anniversary Special – Limited Time

Become TICSA certified for just \$221.25 US when you register before 3/31/03 with PROMO "TS0103" at www.2test.com. NO membership fees, certification good for 2 years. Price for international delivery just \$296.25 US, with this offer. Offer cannot be combined with any other special and expires 3/31/03. Visit www.trusecure.com/ticsa for full details.

oo