

## **-Dokumentation**



### **Zentrum für Informatik ZFI AG**

## **Designing a Secure Microsoft Windows 2000 Network (W2SN) - IT Ausbildung nach Mass**

<http://www.zfi.ch/W2SN>

Weitere Infos finden Sie unter [www.zfi.ch](http://www.zfi.ch) oder via Adresse:

**Zentrum für Informatik ZFI AG  
Zentralsekretariat  
Technoparkstrasse 1  
CH-8005 Zürich  
Telefon: 044 732 40 00  
Telefax: 044 732 40 09**

**Zürich, Basel, Bern, Zürich, Schweiz**

<b>Titel</b>	<b>Designing a Secure Microsoft Windows 2000 Network</b>
<b>Untertitel</b>	
<b>Einleitung</b>	Dieser 4-teilige Kurs vermittelt das Wissen um für kleine wie grosse Unternehmungen sichere Netzwerke mit Windows 2000 Technologie zu gestalten.
<b>Ihr Nutzen</b>	Nach diesem Kurs sind Sie in der Lage (Originalbeschreibung): Identify the security risks associated with managing resource access and data flow on the network. Describe how key technologies within Windows 2000 are used to help protect a network and its resources. Plan a Windows 2000 administrative structure so that permissions are granted only to appropriate users. Plan an Active Directory? directory service structure that facilitates security-enhanced and verifiable user account creation and administration. Define minimum security requirements for Windows 2000?based domain controllers, application servers, file and print servers, and workstations. Design a strategy for to help protect local storage of data and provide security-enhanced network access to file and print resources. Design end-to-end security for the transmission of data between hosts on the network. Design a strategy to help provide security-enhanced access for non-Microsoft clients within a Windows 2000?based network. Design a strategy to help protect local resources accessed by remote users who use dial-up or virtual private network (VPN) technologies. Design a strategy to help protect local resources accessed by remote offices within a wide area network (WAN) environment. Help protect private network resources from public network users. Design a strategy to help protect private network user access to public networks. Design a strategy for authenticating trusted users over public networks. Design a strategy to help protect data and application access for the private network when accessed by trusted partners. Plan for an e-commerce implementation between your organization and external business partners that facilitates business communication. Design a structured methodology for securing a Windows 2000 network
<b>Voraussetzungen</b>	Kenntnisse wie sie in "Implementing and Administering Windows 2000 Directory Services" (ZFI-Kurs: W2ID) vermittelt werden, sind erforderlich.
<b>Teilnehmerkreis</b>	Netzwerkadministratoren, System-Ingenieure, Programmierer
<b>Unterlagen</b>	Original Microsoft (in Englisch, auf Deutsch falls verfügbar)
<b>Folgkurse</b>	
<b>Inhalt</b>	Module 1: Assessing Security Risks Identifying Risks to Data Identifying Risks to Services Identifying Potential Threats Introducing Common Security Standards Planning Network Security Module 2: Introducing Windows 2000 Security Introducing Security Features in Active Directory Authenticating User Accounts Securing Access to Resources Introducing Encryption Technologies Encrypting Stored and Transmitted Data Introducing Public Key Infrastructure Technology Unit 1: Providing Security-Enhanced Access to Local Network Users Module 3: Planning Administrative Access Determining the Appropriate Administrative Model Designing Administrative Group Strategies Planning Local Administrative Access Planning Remote Administrative Access Module 4: Planning User Accounts Designing Account Policies and Group Policy Planning Account Creation and Location Planning

Delegation of Authority Auditing User Account Actions Module 5: Securing Windows 2000? Based Computers Planning Physical Security for Windows 2000? based Computers Evaluating Security Requirements Designing Security Configuration Templates Evaluating Security Configuration Deploying Security Configuration Templates Module 6: Securing File and Print Resources Examining Windows 2000 File System Security Protecting Resources Using DACLs Encrypting Data Using EFS Auditing Resource Access Helping Protect Backup and Restore Procedures Helping Protecting Data from Viruses Module 7: Securing Communication Channels Assessing Network Data Visibility Risks Designing Application-Layer Security Designing IP-Layer Security Deploying Network Traffic Encryption Module 8: Providing Security-Enhanced Access to Non-Microsoft Clients Providing Security-Enhanced Network Access to UNIX Clients Providing Security-Enhanced Network Access to NetWare Clients Providing Security-Enhanced Access to Macintosh Clients Helping to Protect Network Services in a Heterogeneous Network Monitoring for Security Breaches Unit 2: Providing Security-Enhanced Access to Remote Users and Offices Module 9: Providing Security-Enhanced Access to Remote Users Identifying the Risks of Providing Remote Access Designing Security for Dial-Up Connections Designing Security for VPN Connections Centralizing Remote Access Security Settings Module 10: Providing Security-Enhanced Access to Remote Offices Defining Private and Public Networks Helping Protect Connections Using Routers Helping Protect VPN Connections Between Remote Offices Identifying Security Requirements Unit 3: Providing Security-Enhanced Access Between Private and Public Networks Module 11: Providing Security-Enhanced Network Access to Internet Users Identifying Potential Risks from the Internet Using Firewalls to Help Protect Network Resources Using Screened Subnets to Help Protect Network Resources Helping to Protect Public Access to a Screened Subnet Module 12: Providing Security-Enhanced Internet Access to Network Users Helping Protect Internal Network Resources Planning Internet Usage Policies Managing Internet Access Through Proxy Server Configuration Managing Internet Access Through Client-Side Configuration Unit 4: Providing Security-Enhanced Access to Partners Module 13: Extending the Network to Partner Organizations Providing Access to Partner Organizations Securing Applications Used by Partners Securing Connections Used by Remote Partners Structuring Active Directory to Manage Partner Accounts Authenticating Partners from Trusted Domains Module 14: Designing a Public Key Infrastructure Introducing a Public Key Infrastructure Using Certificates Examining the Certificate Life Cycle Choosing a Certification Authority Planning a Certification Authority Hierarchy Mapping Certificates to User Accounts Managing CA Maintenance Strategies Module 15: Developing a Security Plan Designing a Security Plan Defining Security Requirements Maintaining the Security Plan

**Beitrag**

Der Teilnehmerbeitrag versteht sich rein netto. Das ZFI ist (gemäss MwSt-Gesetz) nicht Mehrwertsteuerpflichtig und erhebt somit keine MwSt. Bei länger als einen Monat dauernden Lehrgängen ist die Zahlung des Teilnehmerbeitrages in mehreren Raten möglich (pro rata temporis).