

-Dokumentation



Zentrum für Informatik ZFI AG

Designing Security for Microsoft Networks

(W3SN) - IT Ausbildung nach Mass

<http://www.zfi.ch/W3SN>

Weitere Infos finden Sie unter 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

Titel	Designing Security for Microsoft Networks
Untertitel	Ein Seminar für Sicherheits Spezialisten
Einleitung	Dieser Kurs vermittelt Ihnen das Wissen um eine sichere Netzwerk Infrastruktur zu gestalten. Dazu gehört: assembling the design team, modeling threats, and analyzing security risks in order to meet business requirements for securing computers in a networked environment.Im Kurs wird ein interaktives Tool eingesetzt, das Szenen wie aus dem wirklichen Leben simuliert.
Ihr Nutzen	Nach diesem Kurs sind Sie in der Lage (Originalbeschreibung):Plan a framework for network security.Identify threats to network security.Analyze security risks.Design security for physical resources.Design security for computers.Design security for accounts.Design security for authentication.Design security for data.Design security for data transmission.Design security for network perimeters.Design an incident response procedure.In addition, this course contains three teachable appendices that cover:Designing an acceptable use policy.Designing policies for managing networks.Designing an operations framework for managing security.
Voraussetzungen	Dieser Kurs setzt detaillierte Kenntnisse und Erfahrungen im Umgang mit Windows 2000 oder Windows 2003 voraus, wie sie in den folgenden Kursen vermittelt werden: - "Implementing Microsoft Windows 2000 Professional and Server" (ZFI: W2IM) - "Implementing a Microsoft Windows 2000 Network Infrastructure" (ZFI: W2IN) - "Implementing and Administering Microsoft Windows 2000 Directory Services" (ZFI: W2ID)
Teilnehmerkreis	IT System-Ingenieure und Sicherheits Spezialisten die verantwortlich für die Umsetzung von Sicherheitsrichtlinien und -abläufe in ihrem Unternehmen sind. Der Teilnehmer sollte vorteilhafterweise 1-3 Jahre Berufserfahrung aus diesem Umfeld mitbringen.
Unterlagen Folgekurse	Original Microsoft (in Englisch, auf Deutsch falls verfügbar)
Inhalt	Module 1: Introduction to Designing SecurityIntroduction to Designing Security for Microsoft NetworksContoso Pharmaceuticals: A Case StudyModule 2: Creating a Plan for Network SecurityIntroduction to Security PoliciesDefining a Process for Designing Network SecurityCreating a Security Design TeamModule 3: Identifying Threats to Network SecurityIntroduction to Security ThreatsPredicting Threats to SecurityModule 4: Analyzing Security RisksIntroduction to Risk ManagementCreating a Risk Management PlanModule 5: Creating a Security Design for Physical ResourcesDetermining Threats and Analyzing Risks to Physical ResourcesDesigning Security for Physical ResourcesModule 6: Creating a Security Design for ComputersDetermining Threats and Analyzing Risks to ComputersDesigning Security for ComputersModule 7: Creating a Security Design for AccountsDetermining Threats and Analyzing Risks to AccountsDesigning Security for AccountsModule 8: Creating a Security Design for AuthenticationDetermining Threats and Analyzing Risks to AuthenticationDesigning Security for AuthenticationModule 9: Creating a

Security Design for Data
Determining Threats and Analyzing Risks to Data
Designing Security for Data
Module 10: Creating a Security Design for Data Transmission
Determining Threats and Analyzing Risks to Data Transmission
Designing Security for Data Transmission
Module 11: Creating a Security Design for Network Perimeters
Determining Threats and Analyzing Risks to Network Perimeters
Designing Security for Network Perimeters
Module 12: Designing Responses to Security Incidents
Introduction to Auditing and Incident Response
Designing an Audit Policy
Designing an Incident Response Procedure
Appendices
Appendix A: Designing an Acceptable Use Policy
Analyzing Risks That Users Introduce
Designing Security for Computer Use
Appendix B: Designing Policies for Managing Networks
Analyzing Risks to Managing Networks
Designing Security for Managing Networks
Appendix C: Designing an Operations Framework to Manage Security
Analyzing Risks to Ongoing Network Operations
Designing a Framework for Ongoing Network Operations

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).