

-Dokumentation



Zentrum für Informatik ZFI AG

Designing Security for Microsoft SQL Server

2005 (S9SE) - IT Ausbildung nach Mass

<http://www.zfi.ch/S9SE>

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 SQL Server 2005
Untertitel	Planen der Sicherheit für Microsoft SQL Server 2005
Einleitung	<p>In der heutigen vernetzten Welt müssen Daten und die Systeme zur Verwaltung dieser Daten Ihren Benutzern ständig zur Verfügung stehen. Mit SQL Server 2005 profitieren die Benutzer und IT-Experten der gesamten Organisation von der reduzierten Ausfallzeit, der verbesserten Skalierbarkeit und Performance sowie der erhöhten Sicherheit. SQL Server 2005 enthält zahlreiche Sicherheits-Verbesserungen wie Datenbank-Verschlüsselung, sichere Standardeinstellungen, Durchsetzung von Passwort-Richtlinien, feingranulare Kontrolle von Berechtigungen und ein verbessertes Sicherheitsmodell. Das neue Sicherheitsmodell von SQL Server 2005 verfolgt eine Trennung von Benutzern und Objekten und ermöglicht eine bessere Kontrolle über den Datenzugriff. Darüber hinaus werden alle Systemtabellen als Ansichten implementiert, sodass eine größere Kontrolle über Datenbank-Systemobjekte möglich wird. Dieser ZFI/Microsoft-Kurs befähigt Datenbank-Administratoren, die Sicherheit im Bereich der SQL Server 2005 Datenbanken zu gewährleisten. Dabei wird ein ganzheitlicher Ansatz verwendet, welcher die ganze Umgebung berücksichtigt, von den Geschäfts-Erfordernissen angefangen über Vorschriften des Gesetzgebers, über die Netzwerke bis hin zum Sicherheits-technisch richtigen Design der Datenbanken. Die Teilnehmenden lernen auch, die Sicherheit zu überwachen und auf Bedrohungen entsprechend richtig zu reagieren.</p>
Ihr Nutzen	
Voraussetzungen	<p>Before attending this course, students must: Have basic knowledge of security protocols and how they work. For example, Windows NT LAN Manager (NTLM) or Kerberos. Have basic knowledge of public key infrastructure (PKI) systems. For example, how public and private keys work, strengths and weaknesses, and what they are used for. Have working knowledge of network architectures and technologies. For example, how a firewall works, how IPsec works in a networking context, and common vulnerability points. Have working knowledge of Active Directory directory service. For example, security models, policies, group policy objects (GPOs), and organizational units (OUs). Be able to design a database to third normal form (3NF) and know the tradeoffs when backing out of the fully normalized design (denormalization) and designing for performance and business requirements in addition to being familiar with design models, such as Star and Snowflake schemas. Have strong monitoring and troubleshooting skills. Have experience creating Microsoft Office Visio drawings or have equivalent knowledge. Have strong knowledge of the operating system and platform. That is, how the operating system integrates with the database, what the platform or operating system can do, interaction between the operating system and the database. Have basic knowledge of application architecture. That is, different methods of implementing security in an application, how applications can be designed in three layers, what applications can do, the interaction between applications and the database, and interactions between the database and the platform or operating system. Have knowledge about network security tools. For example, sniffer and port scanning. Must understand how they should be</p>

used. Be able to use patch management systems. Have knowledge of common attack methods. For example, buffer overflow, and replay attacks. Be familiar with SQL Server 2005 features, tools, and technologies. Have a Microsoft Certified Technology Specialist: Microsoft SQL Server 2005 credential or equivalent experience. In addition, it is recommended, but not required, that students have completed: Course SST9/2778: Writing Queries Using Microsoft SQL Server 2005 Transact-SQL. Course S9IM/2779: Implementing a Microsoft SQL Server 2005 Database. Course S9MA/2780: Maintaining a Microsoft SQL Server 2005 Database.

Teilnehmerkreis

This course is intended for current professional database administrators who have three or more years of on-the-job experience administering SQL Server database solutions in an enterprise environment.

Unterlagen

Original Microsoft Kursunterlagen

Folgekurse**Inhalt**

- Introduction to Designing SQL Server Security
- Principles of Database Security
- Methodology for Designing a SQL Server Security Policy
- Monitoring SQL Server Security

- Designing a SQL Server Systems Infrastructure Security Policy
- Integrating with Enterprise Authentication Systems
- Developing Windows Server-Level Security Policies
- Developing a Secure Communication Policy
- Defining SQL Server Security Monitoring Standards
- Lab: Designing a SQL Server Systems Infrastructure Security Policy
- Lab: Creating an Infrastructure Security Inventory

- Designing Security Policies for Instances and Databases
- Designing an Instance-Level Security Policy
- Designing a Database-Level Security Policy
- Designing an Object-Level Security Policy
- Defining Security Monitoring Standards for Instances and Databases
- Lab: Designing Security Policies for Instances and Databases
- Lab: Validating Security Policies for Instances and Databases

- Integrating Data Encryption into a Database Security Design
- Securing Data by Using Encryption and Certificates
- Designing Data Encryption Policies
- Determining a Key Storage Method
- Lab: Integrating Data Encryption into a Database Security Design

- Designing a Security Exceptions Policy
- Analyzing Business and Regulatory Requirements
- Determining the Exceptions and their Impact
- Lab: Designing a Security Exceptions Policy

- Designing a Response Strategy for Threats and Attacks
- Designing a Response Policy for Virus and Worm Attacks
- Designing a Response Policy for Denial-of-Service Attacks
- Designing a Response Policy for Internal and SQL Injection Attacks
- Lab: Designing a Response Strategy for Threats and Attacks

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).