S E M I N A R E

Microsoft

2081

SQL Server Sicherheit (MS IT Boot-Camp)

o Zielgruppe

Dieser Kurs ist für alle geeignet die den Datenbankserver vor unerlaubten Zugriff schützen müssen.

o Voraussetzungen

Grundlegende Kenntnisse SQL Server

o Seminarziel

In diesem 3-tägigen IT-Boot-Camp vermitteln wir Ihnen nicht nur die theoretischen Kenntnisse um den SQL Server zu schützen. Wir führen in einer Vielzahl von praxisrelevanten Übungen die Implementierung von Schutzmaßnahmen auch durch. Die Themen gliedern sich in die Bereichen SQL Server Dienst sichern, Benutzerhandling, Verschlüsselung der Daten und Verbindungen, Angriffe und Injektion sowie Überwachung. Abgerundet wird das Seminar durch einen Einblick in die SQL Server Forensik.
Der Stoff wird in Form von Vorträgen, Demonstrationen, Übungen am System vermittelt. Der Intensivkurs schließt betreute Übungs- und Nachbereitungsphasen nach Seminarende ein. Im Preis enthalten sind außerdem die Übernachtungs- und Verpflegungskosten sowie die Schulungs-unterlagen.

o Seminarinhalt

Sichern von Server und Netzwerk
- Einleitung
- Auswählen eines Kontos für das Ausführen von SQL Server
- Verwalten von Dienst-SIDs
- Verwenden eines verwalteten Dienstkontos
- Verwenden eines virtuellen Dienstkontos
- Verschlüsselung der Sitzung mit SSL
- Konfigurieren einer Firewall für den SQL Server-Zugriff
- Deaktivieren des SQL Server-Browsers
- Nicht benötigte Dienste beenden
- Verwenden von Kerberos für die Authentifizierung
- Verwenden des erweiterten Schutzes, um Angriffe auf Authentifizierungsrelais zu verhindern
- Verwenden transparenter Datenbankverschlüsselung
- Sichern des verbundenen Serverzugriffs
- Konfigurieren der Endpunktsicherheit
- Begrenzung der Funktionalitäten - xp_cmdshell und OPENROWSET

Benutzerauthentifizierung, Autorisierung und Sicherheit
- Einleitung
- Auswahl zwischen Windows- und SQL-Authentifizierung
- Erstellen von Anmeldungen
- Schutz Ihres Servers vor Brute-Force-Angriffen
- Begrenzung der Administratorrechte des SA-Kontos
- Verwenden fester Serverrollen
- Berechtigungen für granularen Server
- Erstellen und Verwenden von benutzerdefinierten Serverrollen
- Erstellen von Datenbankbenutzern und Zuordnen zu Anmeldungen
- Verhindern von Logins und Benutzern, Metadaten zu sehen
- Erstellen einer enthaltenen Datenbank
- Korrigieren von Benutzer - Login - Mapping - Fehlern bei wiederhergestellten Datenbanken

Schützen der Daten
- Einleitung
- Berechtigungen verstehen
- Zuweisen von Berechtigungen auf Spaltenebene
- Erstellen und Verwenden von Datenbankrollen
- Anwendungsrollen erstellen und verwenden
- Verwenden von Schemata für die Sicherheit
- Verwalten von Objektbesitz

CONSULTING & INFORMATIONSDIENSTE GMBH

Erfurt
Michaelisstraße 13a
99084 Erfurt
Tel.: 03 61 / 5 65 93 - 0
Fax: 03 61 / 5 65 93 - 10

München
Berghamer Straße 14
85435 Erding
Tel.: 0 81 22 / 97 40 - 0
Fax: 0 81 22 / 97 40 - 10

Internet
www.md-consulting.de

E-Mail
info@md-consulting.de

Bankverbindung
HypoVereinsbank
Erfurt

IBAN:
DE84 8202 0086
0003 9840 95

SWIFT/BIC:
HYVEDEMM 498

Geschäftsführer
Dr. Martin Diestelmann

HRB Jena 105046

USt.Id Nr.:
DE 150 108 446

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2081

- Schutz von Daten durch Ansichten und gespeicherte Prozeduren
- Konfigurieren von datenbankübergreifender Sicherheit
- Verwalten der Sichtbarkeit des Ausführungsplans
- Verwenden von EXECUTE AS zum Ändern des Benutzerkontexts

Code und Datenverschlüsselung

- Einleitung
- Verwenden von Dienst- und Datenbank-Master-Schlüsseln
- Erstellen und Verwenden symmetrischer Verschlüsselungsschlüssel
- Erstellen und Verwenden von asymmetrischen Schlüsseln
- Erstellen und Verwenden von Zertifikaten
- Daten mit symmetrischen Schlüsseln verschlüsseln
- Daten verschlüsseln mit asymmetrischen Schlüsseln und Zertifikaten
- Erstellen und Speichern von Hash-Werten
- Daten unterzeichnen
- Authentifizierung der gespeicherten Prozedur durch Signatur
- Verwenden von Modulsignaturen zum Ersetzen der datenbankübergreifenden Besitzverkettung
- Verschlüsseln von SQL-Code-Objekten

Kampfangriffe und Injections

- Einleitung
- Definieren der Codezugriffssicherheit für .NET-Module
- Schützen von SQL Server gegen Denial of Service
- SQL Server gegen SQL-Injection schützen
- Sichern von dynamischem SQL aus Injektionen
- Verwenden einer SQL-Firewall oder einer Webanwendungsfirewall

Sicherungswerkzeuge und hohe Verfügbarkeit

- Einführung
- Auswahl des richtigen Kontos für SQL Agent
- Benutzer können ihre eigenen SQL-Agent-Aufträge erstellen und ausführen
- Erstellen von SQL-Agent-Proxys
- Einrichten der Transportsicherheit für Service Broker
- Einrichten der Dialogsicherheit für Service Broker
- Sicherung der Replikation
- Sichern von SQL Server-Datenbankspiegelung und AlwaysOn

Auditierung

- Einleitung
- Verwenden des Profilers zum Überprüfen des SQL Server-Zugriffs
- Verwenden des DML-Triggers für die Prüfung der Datenänderung
- Verwenden von DDL-Triggern für die Prüfung der Strukturänderung
- Konfigurieren der SQL Server-Überwachung
- Auditing und Tracing von benutzerdefinierbaren Ereignissen
- Konfigurieren und Verwenden von Common Criteria Compliance
- Verwenden von System Center Advisor zur Analyse Ihrer Instanzen
- Verwenden des SQL Server Best Practice Analyzers
- Verwenden von Policy Based Management

Einführung in de SQL Server Forensik

o **Seminardauer: 3 Tage**

Lernen im Schulungshotel Gröbern am See in Muldestausee/Gröbern, in der Dübener Heide:
Seminardauer: Erster Tag ab 10:00 Uhr bis letzter Tag ca. 15:00 Uhr
Kleine Gruppen mit 2-4 Teilnehmer (max. 6)
Im Preis enthalten sind:

- Übernachtungskosten im Hotel
- Vollverpflegung inkl. Getränke
- Schulungsunterlagen
- täglich open end
- intensive Übungs- und Nachbereitungsphasen nach Seminarende
- zertifizierter Trainer für MS SQL Server

o **Preis pro Person: 1.990 EUR netto**