

## JAVA EE- UND SOA-SECURITY

Schutz vor Hacker-Angriffen

Dauer: 3 Tage

Nr.: 33059

Durchführungsart: Präsenztraining

Preis: 1.620€ netto / 1.927,80 € inkl. 19 % MwSt.

Zielgruppe: Projektleiter, Software-Ingenieure, Sicherheitsexperten, Administratoren.

Schulungsmethode: Vortrag, Diskussion, Praktikum am System.

Voraussetzungen: Gute Kenntnisse und Erfahrung in der Entwicklung von Web-Anwendungen.

Dieses Seminar wendet sich an Administratoren und Entwickler, die ihre Java Enterprise- und SOA-Anwendungen gegen interne und externe Hackerangriffe schützen wollen. Die Kenntnis der Angriffstechniken ist die Grundvoraussetzung für die erfolgreiche Abwehr von Hackern. Deshalb liegt der Schwerpunkt des Seminars nicht auf theoretischen Betrachtungen, sondern es werden Sicherheits- und Abwehrstrategien sowie deren Umsetzung an konkreten Beispielen im Java-Umfeld herausgearbeitet.

[Voraussetzungstest zu diesem Seminar](#)

[Besuchen Sie unseren Java Blog.](#)

### Programm

Überblick Enterprise Sicherheit:

Sicherheitsrelevante Aspekte der Web Server-Laufzeitumgebung - Applikationssicherheit - OWASP Top-10

Security-Probleme in Java Code:

Injection (SQL, LDAP, XPATH, XML) - Cross Site Scripting - Besonderheiten bei der Verwendung von Java Reflection - Ausnutzen von Konfigurationsfehlern - Bekannte Fehler bei der Benutzung von Frameworks (JPA, Web Frameworks, Web Services, ...)

Java Security:

Subject, Principal, Credential - Keystores - Cryptography-API - Security Policies - Realms - Wie Hacker eine EJB-Anwendung angreifen - Rollen und das EJB-Sicherheits-API - WS Security und WS Policy

Abwehr:

Sicheres Session Management - Absicherung von JDBC - SOA-Security - Integration der Security-Problematik in die Anwendungsentwicklung: Code Reviews, Auditing - Architektur- und Design-Betrachtungen - Security-Patterns für Java - Werkzeuge und Verfahren zur Durchführung von Security-relevanten Tests - Konfiguration und Administration der Server-Plattform am Beispiel von Tomcat und JBoss

