

Microsofts Webserver - Internet Information Server - ist in der aktuellen Version IIS7 in Windows Server 2008 sowie Windows Vista enthalten.

Ihr Nutzen

Nach dem Seminar können Sie potentielle Sicherheitsrisiken in Ihren Web-Applikationen sowie im Webserver erkennen und beseitigen.

Preis pro Teilnehmer

EUR 1920,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Seminarinhalte

1. Tag
 - * Einführung in Web Sicherheit
 - Das STRIDE Model
 - Der Design Prozess für sichere Anwendungen
 - * Konfigurieren eines sicheren IIS 7.0-Webservers
 - Anwendungs-, System-, Diagnose- und HTTP-Features
 - Leistung, Sicherheit und SMTP-Features
 - * Konfigurieren von Websites und Anwendungspools
 - * Konfigurieren von Anwendungseinstellungen
 - Konfigurieren der ASP.NET-Sicherheit
 - * Sichern der Webserver und Websites für IIS 7.0
 - Konfigurieren der Protokollierung für IIS 7.0
2. Tag
 - * Windows Authentifizierung
 - LM, NTLMv2
 - NTLMSSP und SSPI
 - Session Security
 - Kerberos v5
 - * Authentifizierung mit Internet Information Services
 - Web Client Authentication
 - Access Permissions am Web-Server
 - Wahl einer Authentifizierungsmethode
 - Prozesse und Services im User-Context
 - * IIS und ASP.NET
 - Integration in den IIS
 - Kompilierungsmodell
 - ISAPI Filter
 - ASPNET.DLL, HTTP Handler
 - Hierarchie der Konfigurationsdateien
3. Tag
 - * Role-Based Security in ASP.NET
 - Windows Based Authentication versus Forms-Based Authentication
 - Autorisierung von User und Rollen in ASP.NET
 - * Code Access Security in ASP.NET
 - Grundlagen der CAS
 - Verwenden von CAS in Web-Anwendungen
 - Konfigurieren/Anpassen von Code Access Permissions
 - * Sichern von Dateizugriffen
 - Windows Access Controls
 - ACLs setzen
 - Isolated Storage einsetzen
 - * Überprüfen von Benutzereingaben

Voraussetzungen

Kenntnisse der Web-Entwicklung mit ASP bzw. ASP.NET

Hinweise

Version:

- Arten von User-Input-Attacks
- 4. Tag
 - * Sichern von SQL Server - Daten
 - SQL Connections sichern
 - SQL Server Role-Based Security
 - SQL Injection Attacks
 - * Schützen von Kommunikations-Privatsphäre und Datenintegrität
 - Einführung in Kryptographie
 - Arbeiten mit Zertifikaten
 - SSL/TLS Protokolle
 - * Verschlüsseln, Hashing und Signieren im praktischen Einsatz
 - CAPICOM und Cryptography Namespace
 - Digitale Signaturen
 - * Testen der Sicherheit von Web-Anwendungen

