

# Sicherheit von Web-Applikationen

## Ihre Ziele!

- ◆ Datenmissbrauch verhindern
- ◆ Technische und organisatorische Fehler vermeiden
- ◆ Schutzmechanismen implementieren

## Wichtige Schutzmechanismen

- ◆ Sicherheitsanalysen von Web-Applikationen
- ◆ Ableitung von Bedrohungsszenarien
- ◆ Differenzierung von Authentisierungsmethoden
- ◆ Mehrstufiges Security-Modell zum Schutz vor bekannten und unbekanntem Angriffen

## Wirksamkeit und Einsatz von Web Application Firewalls (WAF)

- ◆ Live-Demonstrationen und Penetrationstests typischer Angriffe
- ◆ Anforderungen und Auswahlverfahren von WAFs
- ◆ Installation und Integration in die vorhandenen Systeme
- ◆ Aufwand und Nutzen im Vergleich

## So urteilen Teilnehmer über Management Circle Seminare:

- ◆ „Sehr schlüssig aufgebaute Vorträge!“
- ◆ „Rundum kompetente Referenten!“
- ◆ „Viele neue und nützliche Anregungen für meine tägliche Arbeit!“

## Ihr Praxis-Plus!

- ✓ Live-Demo: Umgehung von Login-Prozessen, Cross-Site Scripting, Cookie Tampering und SQL Injection
- ✓ Praxisbericht: Auswahl und Implementierung einer WAF bei der BV Zahlungssysteme GmbH
- ✓ Applikationssicherheit bei serviceorientierten Architekturen (SOA)

## Ihre Referenten:



Matthias Forster  
**DETACK GmbH**



Thomas Kohl  
**Deny All**



Ulrich Mohr  
**AAAware Consulting**



Ulrich Neider  
**DETACK GmbH**



Dirk Pieck  
**BV Zahlungssysteme GmbH**



Julian Totzek  
**Deny All**

Hoher Lernerfolg durch begrenzte Teilnehmerzahl!

Bitte wählen Sie Ihren Termin:

- 8. und 9. Oktober 2007 in Düsseldorf
- 12. und 13. November 2007 in Frankfurt am Main
- 10. und 11. Dezember 2007 in München

# Verwundbarkeiten von Web-Anwendungen & Typische Angriffsszenarien

Ihr Seminarleiter:

Ulrich Neider, Geschäftsführer, **DETACK GmbH**, Ludwigsburg

**ab 8.30 Uhr** Empfang mit Kaffee und Tee,  
Ausgabe der Seminarunterlagen

## 9.00 Herzlich Willkommen!

## 9.20 Typische Web-Anwendungen und deren Bedrohungspotenziale

- Web-Server, Datenbank-Server, Netzwerk, DMZ, Middleware, LAN und Anmeldeverfahren
- Risikoanalyse und Festlegung von Schutzmaßnahmen
- Bestandsaufnahme und Sicherheitsanalyse von Web-Applikationen
- Ableitung von Bedrohungsszenarien

## Zielsetzungen des Sicherheitsmanagements bei Anwendungen

- Sensibilisierung der Bedeutung von Anwendungssicherheit für alle Bezugsgruppen
- Design, Build and Run – Beitrag der Bezugsgruppen
- Allokation von Budget (monetär und zeitlich) für sichere Programmierung, sicheres Design und Architektur
- Qualitätsmanagement
- Erweiterung der Schutzmechanismen
- Lebenszyklus einer Anwendung

Ulrich Neider

11.00 Kaffee- und Teepause

## 11.30 Grundlagen der Anwendungssicherheit – Strategische Zugriffssteuerung auf Anwendungen

- Öffentliche Erreichbarkeit von Web-Anwendungen
- Verschiedene Techniken zur Zugriffsbeschränkung – Strategien der Risikominimierung
- Konzept „Trust-Level“ – Differenzierung der Authentisierungsmethoden je nach Nutzergruppe
- Gefahr von Interessenskonflikten
- Grundregeln für statische Passwörter

Matthias Forster

Business Development Manger,  
**DETACK GmbH**, Ludwigsburg

12.30 Gemeinsames Mittagessen

## 14.00 Applikationssicherheit bei serviceorientierten Architekturen

- SOA: Web Services (WS) und XML
- Bedrohungen und Content Security
- Grundlegende Security-Anforderungen: State-of-the-Art-Lösungsansätze
- Spezifikationen und Stand der Standardisierung

- WS-Trust und WS-Federation: Reality Check
- Management und Compliance
- SOA Security Marktübersicht und Positionierung europäischer Lösungen
- Ausblick 2008+

Ulrich Mohr

**AAAware Consulting**, Dietzenbach

15.00 Kaffee- und Teepause

## 15.15 Wie laufen Angriffe gegen Anwendungen ab?

- Vorgehensmodell und Grundprinzipien
- Stufen einer Penetration
- Grundprinzipien der Angriffsmethoden – Was „verleitet“ einen Angreifer?
- Fortsetzung der Angriffe nach Innen  
Ziele: Datenbanken, zentrale Dienste wie ADS, LDAP, Management Consolen, etc.

## 16.00 Typische Verwundbarkeiten bei Web-Anwendungen

- Gefahrenpotenziale und Lösungsansätze
- Worst Case-Szenario
- Typische Fehler
- Beispiele für Angriffsszenarien auf Web-Anwendungen
- Direkter Zugriff auf Anwendungsdienste unter Umgehung der Authentifizierung

Ulrich Neider

## 16.45 Fast Track zum Erfolg – Fallbeispiele erfolgreicher Penetration von Anwendungen

- Drei Unternehmen: SAP-Portal Händler, E-Business Industrie und E-Banking-Anwendung
- Was haben alle Fälle gemeinsam?
- Wo unterscheiden sich die Fälle?
- Schlussfolgerungen für Ihr Unternehmen

Matthias Forster

17.30 Zusammenfassung der Ergebnisse des ersten Seminartages durch den Seminarleiter und Gelegenheit zur Diskussion

17.45 Ende des ersten Seminartages und Get-Together

### Get-Together

Ausklang des ersten Seminartages in informeller Runde. **Management Circle** lädt Sie zu einem kommunikativen Umtrunk ein. Entspannen Sie sich in angenehmer Atmosphäre und vertiefen Sie Ihre Gespräche mit den Referenten und den Teilnehmern!

# Schutzmechanismen für Applikationen und Portale & Web-Applikations-Firewall in die Systeme integrieren

Ihr Seminarleiter:  
Ulrich Neider

### 9.00 Es geht weiter!

- Begrüßung durch den Seminarleiter
- Rückblick auf den ersten Seminartag
- Diskussion offener Fragen
- Überleitung zu den Themen des zweiten Seminartages

### Security Audits: Notwendigkeit und Verfahren

- Gründe für Sicherheitsaudits
- Typische Gründe der Ablehnung von Audits
- Organisatorische Lernerfahrungen durch Audits
- Audits als Teil der IT-Sicherheitsstrategie
- Audittypen und Verfahren
  - automatisiert, automatisiert und händisch, Fokus manuelle Methoden
- Pro und Contra

Ulrich Neider

10.40 Kaffee- und Teepause

### 11.00 Schutzmechanismen für webbasierte Applikationen und Portale

- Integration einer WAF-Lösung in die bestehende Infrastruktur
- Mehrstufiges Security-Modell zum Schutz vor:
  - bekannten
  - unbekanntem Angriffen
- Absicherung von Web-Portalen
- Integrierter WAF-Ansatz für SOA-Umgebungen
- Allgemeine Darstellung einer WAF – aus Sicht eines Anbieters

Thomas Kohl  
Business Development Manager,  
**Deny All**, Frankenthal

12.00 Gemeinsames Mittagessen

Live-Demo!

### 13.30 Wirksamkeit einer WAF anhand von Angriffsszenarien

- Erklärung Aufbau der Testumgebung
  - Web-Server
  - WAF
  - Lokaler Proxy
- Der Webserver
  - Was kann ich hier machen?
  - Wie könnte ich angreifen?
- Durchführung der Angriffe
  - Umgehen des Login-Prozesses
  - Cross-Site Scripting
  - komplexe SQL Injection
  - Cookie Tampering
  - Parameter Tampering

- Aufschalten der Security
  - Schrittweise hochfahren der Security
  - Ansicht der Angriffe in den Logs
- Einschätzung der einmaligen und wiederkehrenden Aufwände, wie Administration, Schutz weiterer Anwendungen
- Do's und Don'ts – vor und nach Einführung einer WAF
- Allgemeine Diskussion und Fragen

Julian Totzek  
Technical Consultant,  
**Deny All**, Frankenthal

15.00 Kaffee- und Teepause

### 15.30 „Web Application Firewalls – Ein Erfahrungsbericht“

Praxisbericht!

- Anforderungen
- Auswahlverfahren einer WAF
  - Kandidatentest
  - Auswertung
  - Entscheidung
- Prozessintegration
- Application Lifecycle
  - (Security) Incident Management
  - Nachträgliche Prozessintegration
- Installation, Integration & Deployment
- Mögliche Topologien
- Aufbau einer Sicherheitsleitlinie (Security Policy)
- Planung
  - Notwendige Personen und Skillprofile
  - Analyse der Anwendung
  - Erfahrungen und Grenzen: Was geht, was geht nicht?
- Forum für DBA & SQL Injection
  - Verschlüsselung & WAF
  - Testbetrieb
- Testfälle & hilfreiche Techniken
  - Erfahrungen
  - Produktiver Betrieb
  - Personal
  - Anwendungstypen
  - Policy-Verletzungen
  - Reporting
  - Änderungen
  - Probleme & Erfahrungen
- Fazit

Dirk Pieck  
Zentrale IT,  
**BV Zahlungssysteme GmbH**, Köln

16.45 Zusammenfassung der Inhalte des zweiten Seminartages und Gelegenheit für Ihre abschließenden Fragen

17.15 Ende des Intensiv-Seminars

# Warum dieses Seminar wichtig für Sie

Sobald Sie eine **Web-Applikation** oder **E-Business-Anwendung** betreiben, müssen Sie Ihre Applikationen **sicher vor Angriffen** schützen. Die meisten IT-Manager gehen davon aus, dass sie die Sicherheitsrisiken voll im Griff haben. Doch da liegt ein fataler Irrtum vor. Die üblichen Schutzmechanismen können in den meisten Fällen die **Sicherheitslücken** weder erkennen noch verhindern.

Defizite in der Applikationssicherheit führen zu gezielter URL-Manipulation, eingeschleusten Systemkommandos und Angriffen auf Authentifizierungsprozesse. Kritische Unternehmensdaten können schnell und einfach unbemerkt entnommen und missbraucht werden.

**Schützen Sie sich proaktiv und langfristig von Datenausspähung, Datenmanipulation, Identitätsdiebstahl und Wirtschaftsspionage!**

## Aktuelle Fragestellungen:

- **Welchen Bedrohungspotenzialen sind Ihre Web-Applikationen ausgesetzt?**
- **Wie erfolgen typische Angriffe durch Angreifer?**
- **Welche Fehler müssen vermieden werden, um die Applikationssicherheit zu gewährleisten?**
- **Welche Möglichkeiten bietet der Einsatz einer Web Application Firewall?**
- **Welche technischen und organisatorischen Vorkehrungen müssen Sie initiieren?**

## Konkrete Antworten:

Sie erfahren, welche **Risiken bei Web-Applikationen** auftreten und wie Sie gravierende **Sicherheitsprobleme** für Ihr Unternehmen **vermeiden**. Detailliert erläutern Ihnen unsere Experten, auf welchen Ebenen - **vom Netzwerk bis zur Absicherung von Prozessen** - Sie für sichere Web-Anwendungen sorgen können. Anhand von **typischen Angriffsszenarien** lernen Sie, nach welchen Grundprinzipien **Penetrationen Ihrer Systeme ablaufen** und welche Methoden dabei am häufigsten zum Einsatz kommen. Dafür werden Ihnen **drei praktische Fallbeispiele erfolgreicher Angriffe** vorgestellt. Informieren Sie sich, wie Sie **Designfehler auf Netzwerk- und Applikationsebene vermeiden** und wie Sie sinnvolle **administrative** und **organisatorische Voraussetzungen** schaffen.

Um Sicherheitslücken zu schließen, ist der Einsatz einer **Web Application Firewall** sehr sinnvoll. Wir zeigen Ihnen in **Live-Demonstrationen** die Funktionsweise von **Web Application Firewalls** beispielsweise beim **Umgehen von Login-Prozessen, komplexen SQL Injections** und **Cross-Site Scripting**. Erfahren Sie, wie Sie die richtige **WAF** für Ihr Unternehmen **auswählen** und in Ihren Systemen **implementieren**. Hören Sie, mit welchen einmaligen und wiederkehrenden **Aufwänden** Sie rechnen müssen und was Sie beim **laufenden Betrieb** einer WAF beachten sollten.

## Sie haben noch Fragen? Gerne!



Anne-Barbara Menninger

Anne-Barbara Menninger

Konferenz Managerin

Tel.: 0 61 96/47 22-613

E-Mail: menninger@managementcircle.de

**Matthias Forster** ist Business Development Manager bei der DETACK GmbH in Ludwigsburg. Das Tätigkeitsfeld von Matthias Forster erstreckt sich auf das Projektmanagement im Bereich der IT-Sicherheit für **Großunternehmen im nationalen und internationalen Markt**. Hauptfelder sind hierbei Single-Sign On und Identity Management als Beitrag zur Absicherung des SAP-Umfeldes sowie der damit verbundenen IT-Infrastruktur.

**Thomas Kohl** ist Business Development Manager bei **Deny All** in Frankenthal für die Märkte Deutschland, Österreich und die Schweiz zuständig. Seine Schwerpunkte liegen in der Umsetzung des für Deutschland erfolgreich realisierten Business Modells für die Security-Lösungen im österreichischen und schweizer Markt. Thomas Kohl trägt darüber hinaus die Verantwortung für internationale Key-Accounts außerhalb des eigentlichen Verantwortungsbereiches. Bis 2005 entwickelte Thomas Kohl das Business Modell für die Security-Lösungen von Deny All inklusive der Marktpositionierung, der Vertriebsstrategie und dem Partnerkonzept.

**Ulrich Mohr** ist Inhaber der 2005 gegründeten **AAAware Consulting**. Deren Schwerpunkt ist die Beratung von Unternehmen bei der Umsetzung von innovativen IT-Security Lösungen. Zuvor war Ulrich Mohr seit 2002 als Vertriebsleiter bei der Controlware GmbH tätig. Sein Verantwortungsbereich umfasste dort den Vertrieb sowie das operative Geschäft in Deutschland und Österreich. Seine TK- und IT-Erfahrungen sammelte Ulrich Mohr unter anderem als Geschäftsführer der Cellware Breitband GmbH und als Direktor Strategie der ADVA AG Optical Networking.

**Ulrich Neider** ist Geschäftsführer bei der **DETECT GmbH** in Ludwigsburg, die seit 2001 IT-Audits und Sicherheitsberatungen durchführt. Ulrich Neider betreut vorwiegend Großunternehmen im Bereich Finanzdienstleistung, Industrie, öffentliche Verwaltung und koordiniert umfangreiche Auditprojekte hinsichtlich SAP-Security. Er pflegt den Kontakt zu Management und IT-Sicherheitsverantwortlichen der Kunden, um nach Abgabe der Sicherheitsberichte nicht nur an dem Prozess der Beseitigung der Schwachstellen beteiligt zu sein, sondern auch die organisatorischen Reaktionen und Strategien zu begleiten, um eine nachhaltige Steigerung des Sicherheitsniveaus zu erreichen.

**Dirk Pieck** ist als Netzwerkspezialist für die **BV Zahlungssysteme GmbH** in Köln tätig. Zu seinen Verantwortungsgebieten gehört die technische Konzeption von Projektanforderungen bzgl. Netzwerk und IT-Security zur Realisierung eines sicheren und verfügbaren IT-Betriebs. Ein Schwerpunkt seiner Arbeit liegt zusätzlich in der Gestaltung von Prozessen zur permanenten Optimierung interner Abläufe. Er steht den einzelnen Fachabteilungen und Fachbereichen als Berater und Projektleiter zur Verfügung. Für einen mittelständischen Systemintegrator hat er zuvor als „Berater IT-Security“ langjährige Erfahrungen im IT-Umfeld in den unterschiedlichsten Branchen gewinnen können.

**Julian Totzek** ist Technical Consultant bei **Deny All** in Frankenthal und für die Märkte Deutschland, Österreich und die Schweiz zuständig. Seine Aufgabenschwerpunkte umfassen die Presales Beratungen, die Erarbeitung von Speziallösungen, die Installation beim Kunden und der Support von Security-Lösungen. Zuvor sammelte Julian Totzek Erfahrungen als IT-Security Consultant bei The Bristol Group und als Technischer Leiter sowie Webmaster bei der con5 GmbH.

### AUCH ALS INHOUSE TRAINING

#### So individuell wie Ihre Ansprüche – Inhouse Trainings nach Maß!

Zu allen Themenbereichen bieten wir auch firmeninterne Schulungen an. Ihre Vorteile: Kein Zeitverlust – passgenau für Ihren Bedarf!

Ich berate Sie gerne und erstelle Ihnen ein individuelles Angebot. Rufen Sie mich an.



**Dirk Gollnick**

Tel.: 0 61 96/47 22-646

E-Mail: gollnick@managementcircle.de

## Ihre Vorteile auf einen Blick:

- Akute Bedrohungssituationen kennen!
- Typische Angriffsszenarien live erleben!
- Erfolgreiche Schutzmechanismen erfahren!
- Wirksamkeit einer WAF kennen lernen!
- Webbasierte Applikationen und Portale langfristig absichern!
- Live-Demonstrationen und Erfahrungsberichte!

## Wer sollte teilnehmen?

Das Seminar richtet sich an **Leiter IT, IT-Security-Manager, CISOs, CISSPs, CISM, IT-Risikomanager, CIOs, Leiter Rechenzentrum, Leiter Unternehmenssicherheit, Datenschutzbeauftragte**, Verantwortliche für **operationelle Risiken, Systemadministratoren, Netzwerk- und Kommunikationsexperten, E-Business-Manager** sowie **IT-Revisoren und -Auditoren**. Weiterhin angesprochen sind interessierte Unternehmens- und IT-Berater.

## Termine und Veranstaltungsorte

### 8. und 9. Oktober 2007 in Düsseldorf

Holiday Inn Düsseldorf City Centre Königsallee,  
Graf-Adolf-Platz 8-10, 40213 Düsseldorf  
Tel.: 0211/3848-0, Fax: 0211/3848-390  
E-Mail: reservation.hi-duesseldorf-citycentre@queensgruppe.de

### 12. und 13. November 2007 in Frankfurt am Main

Holiday Inn Hotel Frankfurt Airport-North,  
Isenburger Schneise 40, 60528 Frankfurt  
Tel.: 069/6784-0, Fax: 069/6784-190  
E-Mail: reservation.hi-frankfurt-airportnorth@queensgruppe.de

### Airport-Shuttle auf Anfrage

### 10. und 11. Dezember 2007 in München

Sheraton München Westpark, Garmischer Straße 2, 80339 München  
Tel.: 089/5196-0, Fax: 089/5196-803  
E-Mail: westpark@arabellasheraton.com

### Zimmerreservierung

Für die Seminarteilnehmer steht im jeweiligen Tagungshotel ein begrenztes Zimmerkontingent zum Vorzugspreis zur Verfügung. Nehmen Sie die **Reservierung bitte rechtzeitig selbst direkt im Hotel** unter Berufung auf Management Circle vor. Die Anfahrtsskizze erhalten Sie zusammen mit der Anmeldebestätigung.

## So melden Sie sich an

Bitte einfach die Anmeldung ausfüllen und möglichst bald zurücksenden oder per Fax, Telefon oder E-Mail anmelden. Sie erhalten eine Bestätigung, sofern noch Plätze frei sind – andernfalls informieren wir Sie sofort. Die Anmeldungen werden nach Reihenfolge der Eingänge berücksichtigt.

## Ihre Service-Hotlines

### Anmeldung:

**Manuela Rother**

Telefon: 0 61 96/47 22-700 oder  
0 61 96/47 22-0 (Telefonzentrale)  
Fax: 0 61 96/47 22-999

Per Post: Management Circle AG  
Postfach 56 29, 65731 Eschborn/Ts.  
Hauptstraße 129, 65760 Eschborn/Ts.  
E-Mail: anmeldung@managementcircle.de

### Kundenservice:

**Roman Kern**

Telefon: 0 61 96/47 22-800 (Fax: -888)  
E-Mail: kundenservice@managementcircle.de

### Adressänderung:

**Stella Avramidou**

Telefon: 0 61 96/47 22-500 (Fax: -562)  
E-Mail: marketingservice@managementcircle.de

### Ausstellung:

**Michael Vlajic**

Telefon: 0 61 96/47 22-601 (Fax: -444)  
E-Mail: vlajic@managementcircle.de

### Datenschutz-Hinweis:

Sie können bei uns der Verwendung Ihrer Daten widersprechen, wenn Sie in Zukunft keine Prospekte mehr erhalten möchten. (§28 VI BDSG)

Die Teilnahmegebühr für das zweitägige Seminar beträgt inkl. Mittagessen, Erfrischungsgetränken, Get-Together und der Dokumentation € 1.695,-. Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Sollten mehr als zwei Vertreter desselben Unternehmens an der Veranstaltung teilnehmen, bieten wir **ab dem dritten Teilnehmer 10% Preisnachlass**. Bis zu zwei Wochen vor Veranstaltungstermin können Sie kostenlos stornieren. Danach oder bei Nichterscheinen des Teilnehmers berechnen wir die gesamte Tagungsgebühr. Die Stornierung bedarf der Schriftform. Selbstverständlich ist eine Vertretung des angemeldeten Teilnehmers möglich. Alle genannten Preise verstehen sich zzgl. der gesetzlichen MwSt.

## Sicherheit von Web-Applikationen

Ich/Wir nehme(n) teil am:

WS

- 8. und 9. Oktober 2007 in Düsseldorf** 10-55147  
 **12. und 13. November 2007 in Frankfurt/M.** 11-55148  
 **10. und 11. Dezember 2007 in München** 12-55149

**1** NAME/VORNAME \_\_\_\_\_  
 POSITION/ABTEILUNG \_\_\_\_\_

**2** NAME/VORNAME \_\_\_\_\_  
 POSITION/ABTEILUNG \_\_\_\_\_

**3** NAME/VORNAME \_\_\_\_\_  
 POSITION/ABTEILUNG \_\_\_\_\_  
 MITARBEITER:  BIS 100  100-200  200-500  500-1000  ÜBER 1000

FIRMENNAME \_\_\_\_\_

STRASSE/POSTFACH \_\_\_\_\_

PLZ/ORT \_\_\_\_\_

TELEFON/FAX \_\_\_\_\_

### Warum Ihre E-Mail-Adresse wichtig ist!

Sie erhalten so schnellstmöglich eine Bestätigung Ihrer Anmeldung, damit Sie den Termin fest einplanen können.

E-MAIL  
(MIT NENNUNG MEINER E-MAIL-ADRESSE ERKLÄRE ICH MICH EINVERSTANDEN, ÜBER DIESE MEDIUM INFORMATIONEN DER MANAGEMENT CIRCLE GRUPPE ZU ERHALTEN.)

DATUM \_\_\_\_\_ UNTERSCHRIFT \_\_\_\_\_

ANSPRECHPARTNER/IN IM SEKRETARIAT: \_\_\_\_\_

ANMELDEBESTÄTIGUNG BITTE AN: \_\_\_\_\_ ABTEILUNG \_\_\_\_\_

RECHNUNG BITTE AN: \_\_\_\_\_ ABTEILUNG \_\_\_\_\_

Mit der Deutschen Bahn AG zum **Sonderpreis** zur Veranstaltung. Infos unter:  
[www.managementcircle.de/bahn](http://www.managementcircle.de/bahn) Die Bahn

## Über Management Circle

Management Circle steht für **WissensWerte** und ist anerkannter Bildungspartner der Unternehmen. Mit kompetenten Bildungsleistungen garantieren wir durch unsere Erfahrung Fach- und Führungskräften nachhaltigen Lernerfolg. Vom praxisnahen Seminar bis zur richtungsweisenden Kongressmesse – vom individuell konzipierten In-house Training, praxisorientierten schriftlichen Management-Lehrgang bis zum innovativen E-Learning erhalten Sie alles aus einer Hand. Mit über 40.000 Teilnehmern bei unseren Präsenzveranstaltungen im vergangenen Jahr gehört die Management Circle AG zu den Marktführern im deutschsprachigen Raum. Unser aktuelles und vollständiges Bildungsangebot finden Sie unter: [www.managementcircle.de](http://www.managementcircle.de).

Aktuelle Veranstaltungsangebote: [www.managementcircle.de](http://www.managementcircle.de)