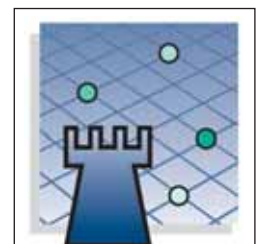


Herausforderung Security!

Im Spannungsfeld zwischen Commodity,
Wertschöpfung und Innovation



14.–15. Februar 2008
Freising bei München
München Airport Marriott Hotel



seckop
2008

VERANSTALTER

FINAKI Deutschland GmbH
Managementkongresse

Franz X. Glas
Vorsitzender der Geschäftsführung

Johanna Gärtner
Iris Vogtmann
Erna Craß
Organisation

Christoph Hecker
Geschäftsführer *CIOcolloquium*

INHALT

Präambel 4

Programmkomitee und Redner 5

Workshops 6 + 7

Programm und Tagungsablauf 8

Charta 9

Veranstaltungsdaten und Konditionen 10

PRÄAMBEL

Liebe SECKOP-Teilnehmer, liebe Geschäftsfreunde,

das Geleitwort für eine Security-Konferenz zu schreiben, bringt es mit sich, aus einer Vielzahl von Studien unangenehme Wahrheiten zu zitieren, Gefährdungsszenarien zu entwerfen, und negative Erfahrungen anzusprechen. Viel lieber würde ich darüber berichten, dass es halb so schlimm ist und am Ende alles gut wird. Aus meiner praktischen Erfahrung als Sicherheitsverantwortlicher weiß ich, dass das allerdings wohl ein Wunschtraum bleiben wird.

Natürlich ist in Sachen Sicherheit in vielen Unternehmen eine Menge passiert und das Bewusstsein für dieses Thema sowohl beim Management, als auch bei den Mitarbeitern in den vergangenen Jahren deutlich gestiegen. Auch gibt es auf dem Markt eine Vielzahl von Produkten und Lösungen, die dem Sicherheitsverantwortlichen helfen, Gefahren frühzeitig zu erkennen und Risiken zu reduzieren. Aber auch die Angreifer schlafen nicht. Die immer gezielteren Angriffe zwingen Unternehmen und Sicherheitsverantwortliche auf neue Bedrohungen immer wieder neue Abwehrstrategien zu finden.

Es besteht kein Zweifel: Der Markt für Security brummt, sehr zur Freude von Herstellern und Beratungsunternehmen, denn Abwehrmaßnahmen gegen Malware oder Hacker-Attacks lassen sich nicht über singuläre Aktionen erledigen. Sie fordern ein kontinuierliches Engagement und eine gesamtheitliche Strategie.

Und genau hier setzen wir mit dem 2. Managementdialog zu Business Continuity, IT-Sicherheit und Ganzheitliche Sicherheit, der SECKOP2008, an. Unter dem Motto „Herausforderung Security! – Im Spannungsfeld zwischen Commodity, Wertschöpfung und Innovation“ treffen sich die Sicherheitsverantwortlichen der Anwenderunternehmen mit den Delegierten wichtiger Anbieter- und Beratungsunternehmen, um sich gemeinsam den Herausforderungen zu stellen und neue Lösungsansätze und Best-Practices zu erarbeiten. Und wie bei den FINAKI-Veranstaltungen üblich, stehen die Workshops im Zentrum der Aufmerksamkeit.

Ich wünsche uns allen eine erfolgreiche Veranstaltung mit fruchtbaren Diskussionen sowie wertvollen Ergebnissen.

Ihr Präsident der SECKOP2008
Dr. Rolf Reinema
Leiter Sicherheit und Datenschutz
Vodafone D2 GmbH

Die Diskussionsplattform

Mit der SECKOP wurde eine branchenneutrale Plattform für die Diskussion aktueller Fragen geschaffen. Es treffen sich dazu die Fraktionen der ITK-Verantwortlichen renommierter Anwenderunternehmen mit den Experten der Anbieter- und Dienstleistungsindustrie.

Das Ziel: der fachlich strategische Diskurs

Anlässlich der SECKOP2008 sollen Antworten zum Leitthema gefunden werden. Dabei werden Zukunftsszenarien unter technischen und wirtschaftlichen Aspekten diskutiert und Eckwerte für Entscheidungsprozesse konkretisiert. Das Ziel wird sein, Positionen zu bestimmen, Chancen und Risiken abzuwägen, sowie neue effektive Wege für eine moderne Infrastruktur und gesicherte Kommunikation in den Unternehmen zu erörtern.

Die Workshops als Kernelemente

Schwerpunkte der Konferenz sind die Roundtable-Gespräche (Workshops). Diese werden – flankiert von Plenarvorträgen – mit fünf Schwerpunktthemen parallel durchgeführt. Die Workshops, die paritätisch mit Vertretern der Anwender- und Anbieterindustrie besetzt sind, werden professionell moderiert und die Resultate dokumentiert. Alle Ergebnisse werden am letzten Tag dem Gesamtplenium präsentiert.

Die Ergebnisse: richtungsweisend

Es werden sicher keine Patentrezepte, jedoch – durch die geballte Fachkompetenz der Anwesenden – Impulse, Anregungen und Weichenstellungen für eine optimierte Unternehmensperformance zu erwarten sein.

Kontakte knüpfen

Darüber hinaus ermöglicht die SECKOP2008 ein persönliches Kennenlernen, fördert den Gedankenaustausch und erleichtert geschäftliche Abstimmungen nach der Konferenz.

Der Initiator der SECKOP2008

FINAKI Deutschland GmbH veranstaltet seit 1997 Managementdialoge für die ITK-Entscheider der großen Unternehmen des deutschsprachigen Raumes (SECKOP, SYSKOP und INKOP). Diese Konferenzen haben sich mittlerweile zu einem Synonym einer hochwertigen und herstellerunabhängigen Arbeitsgemeinschaft auf Topebene entwickelt.

PROGRAMMKOMITEE

Die SECKOP ist eine Arbeitsgemeinschaft auf Toplevel. Die Inhalte wurden vom Programmkomitee entwickelt, das wichtige Branchen des deutschsprachigen Wirtschaftsraumes repräsentiert.

Der Präsident:

Dr. Rolf Reinema
*Leiter Sicherheit und Datenschutz,
Vodafone D2*

Die Mitglieder:

Uwe Fischer
*Technology Manager/ISO,
E.ON*

Dr. Udo Helmbrecht
*Präsident,
BSI*

Detlev Henze
*Geschäftsführer,
TÜV Rheinland Group Secure iT*

Andreas Heutling
*MBCI, Business Continuity Management
Münchner Rückversicherungs-Gesellschaft*

Marcus Rubenschuh
*CISO UB Brief
Deutsche Post*

Monika Wohlrabe
*BCM-Officer,
ASIC Allianz Shared Infrastructure Services GmbH*

Hans-Dieter Stangl
*Geschäftsführer,
netsecure Deutschland (assoziiert)*

REDNER

Zur Eröffnung:
„Security auf dem Weg zur Commodity?!“



Georg Szabo
*Leiter Security Management
Postbank Systems AG*

Zum Abschluss:
„Ausnahmesituation – Arbeiten im Krisenstab“



Axel Bédé
*Kriminaloberrat im Landeskriminalamt Berlin
Chef des Dezernates für „Organisierte Kriminalität“*

WORKSHOPS IM DETAIL

1 Business Continuity und Risk Management

Das Risiko für die unternehmerische Sicherheit und die Geschäftsabläufe wächst aus der Perspektive der IT-Sicherheitsverantwortlichen ständig. Gründe hierfür sind erhöhte Gefahrenpotenziale durch Sabotage, Vandalismus und Terrorismus, die zunehmende Komplexität einzelner Prozesse und der Infrastrukturen sowie nicht zuletzt die immer höhere Zahl der IT-gestützten Prozesse in den Unternehmen. Dies und neue gesetzliche Anforderungen wie SOX, Basel II und KontraG liefern vielfältige Herausforderungen für die verantwortlichen Manager. Es besteht ein klarer Bedarf an umfassenden Business Continuity Konzepten.

Zunächst erfolgt ein professionelles Risk Assessment. Es hilft, mögliche Risiken zu erkennen, sie richtig zu bewerten und damit auch geeignete Maßnahmen zur Prävention, Risikovermeidung, Reduzierung der Schadenshäufigkeit oder -höhe sowie Risikouberwälzung (Versicherungen oder Dienstleistungsvereinbarungen) zu definieren oder auch als nicht vermeidbar per Risk Acceptance zu akzeptieren. Dann sind, dem Risikopotenzial entsprechende, Wiederanlauf- und Notfallpläne zu schaffen.

Das Ergebnis eines solchen Prozesses ist oft eine ganz neue Transparenz im Unternehmen: Welche Prozesse haben den größten Einfluss auf den Unternehmenserfolg? Von welchen Anwendungen, Daten, Menschen und Infrastrukturen hängen diese wirklich ab? Worauf kann wie lange verzichtet werden? Die möglichen Risiken zu kennen, heißt sie beherrschbar zu machen. Da überrascht es nicht, wenn zahlreiche Studien zu dem Ergebnis kommen, dass krisensichere Unternehmen auch in Normalsituationen wirtschaftlich erfolgreicher sind!

Im Workshop werden Beispiele und Lösungsansätze diskutiert und mögliche Handlungsempfehlungen erarbeitet.

Workshop-Leitung: Monika Wohlrabe,
ASIC Allianz Shared Infrastructure Services

Co-Moderation: Hans-Dieter Stangl, netsecure

2 Compliance Management

Ein Compliance-Management, das zu jeder Zeit und in jedem Unternehmensbereich die relevanten externen und internen Regularien und Vorschriften mit der Aufbau- und Ablauforganisation umsetzt, stellt Unternehmen vor große Herausforderungen. Das Wirtschaftsleben wird beherrscht von Unternehmenszusammenschlüssen, Verkäufen von Teilunternehmen oder Personalabbau. Sie alle tragen dazu bei, dass die Compliance eine dauerhafte Baustelle bleibt.

Heute wird Compliance in der Regel einmal konzipiert und selten den sich ständig ändernden Anforderungen angepasst. Gleichzeitig steigen die regulatorischen Anforderungen ständig. Waren es ab 2004 nur US-börsennotierte Unternehmen und deren Tochtergesellschaften, die den Compliance Anforderungen unterworfen waren, so sind es ab dem 1. April 2008 auch alle japanischen Kapitalgesellschaften. Und für Europa gilt die 8. EU-Richtlinie (Euro-SOX), die bis Juni 2008 in nationales Recht umgesetzt werden muss.

Allen diesen Compliance-Standards liegt das gleiche Bestreben zugrunde: Bilanzskandale der Vergangenheit, wie etwa Enron, in Zukunft zu verhindern und das Vertrauen der Investoren wieder herzustellen. Gemein ist allen die zusätzliche Verantwortung des Managements, Risiken in den Unternehmensprozessen zu erkennen, ihnen durch die Implementierung eines internen Kontrollsystems (IKS) im Hinblick auf den Abschluss („over financial reporting“) zu begegnen und jedes Jahr erneut die Wirksamkeit im Design sowie im operativen Geschäft nachzuweisen.

Compliance-Management erstreckt sich von der Managementebene über Finanzprozesse bis hin zur unterstützenden IT. Es stellt ein komplexes, das gesamte Unternehmen durchdringendes Prozesssystem zur Steuerung, Kontrolle, Anpassung und Reporting dar, das ein Höchstmaß an Disziplin fordert. Die IT ist aufgerufen entsprechende Maßnahmen, Verfahren und Tools zur Verfügung zu stellen, um das Corporate Compliance-Management zu unterstützen und möglicherweise steuernd in die Hand zu nehmen.

Im Workshop sollen Handlungsempfehlungen für den Umgang mit Compliance Fragen, insbesondere aus IT-Sicht, erarbeitet werden. Hier werden auch Anforderungen an Compliance Tools und Plattformen ermittelt und Best Practice Beispiele diskutiert.

Workshop-Leitung: Detlev Henze,
TÜV Rheinland Group Secure iT

Co-Moderation: Christoph Hecker, FINAKI Deutschland

Workshopteilnahme und -organisation

Die Workshops laufen zeitlich parallel, d.h. es ist jeweils nur die Teilnahme an einem Workshop möglich. Die Ergebnisse aller Workshops werden dem Gesamtplenium im Rahmen einer InfoFair präsentiert. Der Dialog auf der InfoFair ermöglicht allen Teilnehmern sich über sämtliche Workshopergebnisse detailliert zu informieren.

FINAKI dokumentiert diese Ergebnisse in der Schlussakte.

WORKSHOPS IM DETAIL

3 IT-Sicherheit bei E-Mail und mobilem Einsatz

Die Elektronische Mail (E-Mail) ist aus dem beruflichen wie privaten Alltag nicht mehr wegzudenken. Eine Vielzahl von Informationen wird schnell und bequem über offene elektronische Netze übertragen. Und auch die Anzahl sensibler Informationen nimmt deutlich zu. Die E-Mail eignet sich aber – ohne Schutzmaßnahmen – nicht für die Übertragung sensibler Daten und Informationen: Erstens wird sie in direkt lesbarem Klartext übermittelt. Und zweitens wird die E-Mail über offene Netze von Mailserver zu Mailserver versandt.

Zum Erhalt der Vertraulichkeit und Integrität, werden inzwischen vermehrt kryptographische Schutzmaßnahmen wie Verschlüsselung und elektronische Signatur eingesetzt. Die Einführung dieser Maßnahmen in Behörden- oder Unternehmensstrukturen können sehr unterschiedlich sein. Daher stellt sich bei ihrer Umsetzung die Frage, ob beispielsweise eine Ende-zu-Ende-Verschlüsselung in Einzelfällen ausreicht, oder ob eine Virtuelle Poststelle (VPS) eingesetzt werden sollte. Aber wie können die Mitarbeiter hierfür sensibilisiert werden?

Ebenso normal wie die Nutzung der Elektronischen Mail, ist heute die Nutzung von IT auf Dienst- oder Geschäftsreisen. Doch was bedeutet das für die Sicherheit? Laptops, PDAs und USB-Sticks mit sensiblen Daten werden ohne Sicherheitsbedenken unverschlüsselt über drahtlose Schnittstellen verwendet und dann in Flugzeug, Bahn oder Taxi vergessen. Welche Schutzmaßnahmen bieten sich grundsätzlich an? Lassen sich diese auch dann durchsetzen, wenn unterwegs dadurch ein performantes Arbeiten nicht mehr möglich ist?

Diese und weitere Fragen werden im Workshop diskutiert. Praktische Handlungsempfehlungen werden gemeinsam erarbeitet.

Workshop-Leitung: Dr. Udo Helmbrecht,
Bundesamt für Sicherheit in der IT (BSI)

Co-Moderation: Heinz Altengarten,
Bundesamt für Sicherheit in der IT (BSI)

4 SOA – Security entlang des Geschäftsprozesses

Die Service Orientierte Architektur (SOA) bietet ein intelligentes Bindeglied zwischen ganzheitlicher Geschäftsprozesssicht und den unterstützenden Anwendungen. Indem SOA die Geschäftsprozesse auf die IT-Systeme abbildet, strukturiert sie die verschiedenen Ebenen und lässt sie transparent werden. Gleichzeitig wird damit idealerweise die Komplexität von heterogenen und gewachsenen IT-Landschaften effizient beherrschbar.

Auf der anderen Seite steigt damit zunächst die Angriffsfläche für unerwünschte Eindringlinge drastisch an. Erst durch eine entsprechende weitere Instanz der Absicherung kann dieses Tor geschlossen werden.

So müssen zum Beispiel aus Sicherheitsgründen die Servicegeber den Geschäftsanforderungen an die Informationssicherheit entsprechen. Die Kommunikationselemente der SOA benötigen eine gezielte Absicherung der Kommunikation sowie Authentisierung/Autorisierung von beteiligten Services und die zugrunde liegende Infrastruktur hat erhöhte Anforderungen an die Verfügbarkeit und IT-Sicherheit im Allgemeinen.

Aber auch mögliche Synergieeffekte sind zu nennen. So erhält man durch die zusätzlichen Security Aufwendungen eine erhöhte Informationssicherheit – eine ganz wesentliche Voraussetzung für ein erfolgreiches Business Continuity Konzept.

Eine offene Diskussion über technische Trends und Paradigmenwechsel wird den Teilnehmern helfen von den Kollegen zu lernen, neue Konzepte zu verstehen und gemeinsam vernünftige, ganzheitliche Lösungsansätze zu skizzieren und zu planen

Workshop-Leitung: Uwe Fischer, E.ON

Co-Moderation: Marcus Rubenschuh, Deutsche Post

5 Gelebtes Krisenmanagement (Fallstudie)

Das Krisenmanagement ist ein integraler Bestandteil einer ganzheitlichen Business Continuity Lösung. Durch ein funktionierendes Krisenmanagement werden außerordentliche Führungsprozesse und Managementverfahren definiert, beschrieben und innerhalb der Krisen- und Notfallbewältigung durch die Unternehmensführung oder einen Krisenstab ausgeführt und überwacht. In erster Linie gehören dazu Verfahren zur Lage- und Situationsbeurteilung sowie zur Krisenkommunikation, wie Presse- und Öffentlichkeitsarbeit, Mitarbeiter- und Kundeninformationen sowie das Initiieren, Koordinieren und Überwachen von Recovery-Verfahren.

Anhand eines realistischen Übungs-Szenarios gewinnen die Teilnehmer Einblicke in die Aufgaben und Verantwortlichkeiten eines Krisenstabes in einer derartigen Krisensituation und lernen die Grundlagen von Krisenmanagement innerhalb des BCM-Prozesses kennen.

Im Rahmen der Fallstudie werden die jeweiligen Situationen aus unterschiedlichen Perspektiven beleuchtet (z.B. Kunde, Mitarbeiter, CSO, BCM, Vorstand, Betriebsrat, usw.) und die Potenziale aber auch mögliche Konfliktfelder herausgearbeitet. Mit Rollenspielen, Aufstellungen, etc. werden bei Bedarf Einzelthemen noch weiter vertieft und verschiedene Lösungsszenarien erarbeitet.

Aufgrund der speziellen Arbeitsweise ist die Teilnehmerzahl in diesem Workshop auf 16 Personen begrenzt.

Workshop-Leitung: Andreas Heutling,
Münchner Rückversicherungs-Gesellschaft

Co-Moderation: Uwe Naujoks,
UKN Management Consulting

Wichtig

Die beschriebenen Inhalte sollen als grundsätzliche Basis für die Workshoparbeiten dienen. Die Workshopmitglieder werden sich mit dem Moderatorenteam auf die Schwerpunkte in ihrem Workshop einigen, die sinnvoll bearbeitet werden können.

DONNERSTAG, 14. FEBRUAR 2008

ab 10.00 Uhr

Eintreffen der Teilnehmer und erste Gespräche

10.30 Uhr

Begrüßung durch Franz X. Glas,
Geschäftsführer FINAKI Deutschland

Eröffnung der Konferenz durch den Präsidenten Dr. Rolf Reinema
Leiter Sicherheit und Datenschutz, Vodafone D2

11.00 Uhr

Begrüßungs- und Eröffnungsvortrag:

„**Security auf dem Weg zur Commodity?!**“

Georg Szabo

*Leiter Security Management
Postbank Systems AG*

12.00 Uhr

Einstimmung aller Teilnehmer auf die Workshop-Arbeit und Methodik

12.15–13.30 Uhr

Beginn der Workshop-Arbeit (Teil I)

*(Die Workshops sind paritätisch mit Mitgliedern der Anwenderunternehmen
und Delegierten der ITK-Industrie und -Dienstleister besetzt)*

Die einzelnen Workshops:

- 1 Business Continuity und Risk Management
- 2 Compliance Management
- 3 IT-Sicherheit bei E-Mail und mobilem Einsatz
- 4 SOA – Security entlang des Geschäftsprozesses
- 5 Gelebtes Krisenmanagement (Fallstudie)

13.30 Uhr

Gemeinsames Mittagessen

14.30–19.00 Uhr

Fortsetzung der Workshop-Arbeit (Teil II)

20.00 Uhr

Empfangscocktail
anschließend gemeinsames Abendessen,
Gedankenaustausch, Networking

FREITAG, 15. FEBRUAR 2008

9.00 Uhr

Fortsetzung der Workshop-Arbeit (Teil III)
und Vorbereitung für die InfoFair

10.30 Uhr

Überblick über die Workshop-Ergebnisse,
Kurzpräsentationen im Plenum

11.00 Uhr

InfoFair: offene Diskussion der Workshop-Ergebnisse (walk-around)

12.00 Uhr

Gemeinsames Mittagessen

13.30–14.30 Uhr

Abschlussvortrag

„**Ausnahmesituation – Arbeiten im Krisenstab**“

Axel Bédé

*Kriminaloberrat im Landeskriminalamt Berlin,
Chef des Dezernates für „Organisierte Kriminalität“*

14.30 Uhr

Resümee und Schließung der Konferenz durch den Präsidenten
Bekanntgabe des Termins für die SECKOP2009

anschließend

Ausklang, Gelegenheit für weitere Gespräche

CHARTA

Die SECKOP2008 ist durch die Anwenderunternehmen initiiert. Sie basiert auf Leitsätzen und Spielregeln, die in dieser Charta festgehalten sind.

Die Tagungsinhalte und das Programmkomitee

Die Vertreter der Anwenderunternehmen bestimmen das Programm mit dem Leitthema und den Workshopinhalten. Sie bilden Jahr für Jahr ein Programmkomitee. Die Mitglieder des Komitees repräsentieren einen Querschnitt der Wirtschaftsbranchen. Die Mitgliedschaft im Komitee ist auf maximal zwei Jahre begrenzt. Damit wird ein fließender Wechsel in der Zusammensetzung des Komitees gewährleistet.

Der Präsident

Aus dem Programmkomitee rekrutiert sich der Vorsitzende, der in seiner Eigenschaft als Präsident die Konferenz eröffnet, sie moderiert und schließt.

Die Zusammensetzung der Konferenz

Die Teilnehmer setzen sich paritätisch aus Unternehmen der jeweiligen Wirtschaftssektoren – als Anwender – und Unternehmen der ITK-Industrie – als Anbieter – zusammen. Eine Zusage zur Teilnahme setzt die Bereitschaft zur aktiven Mitarbeit in den Roundtable-Diskussionen voraus.

Die Teilnehmer selbst

Die Anwenderunternehmen entsenden ihren ITK-Chef oder ihren Businessmanager, je nach Schwerpunkt ihres Kerngeschäfts. Sie werden den Mitgliedern des Managements und Technologieexperten der ITK-Anbieter gegenüber sitzen.

Teilnehmerbeschränkung

Die Gesamtzahl aller Konferenzteilnehmer ist auf 120 Personen beschränkt. Diese Beschränkung gewährleistet Transparenz und effektives Arbeiten in den Workshops.

Der Konferenzstil

Die FINAKI-Konferenzen sind geprägt durch ihren herstellerunabhängigen und streng neutralen Charakter. Vertriebs- und Marketingaktivitäten vor Ort sind ausgeschlossen. Hervorzuheben ist die sachliche aber auch freie und ungezwungene Atmosphäre, in der die Konferenzen stattfinden. Für die Tagesarbeit und die Abende ist Freizeitkleidung erwünscht.

Die Finanzierung

Den Hauptteil der Konferenzkosten sponsert die ITK-Industrie durch ihre Teilnahmegebühr, während die Anwenderunternehmen die Selbstkosten tragen. Die Teilnehmer können sich deshalb frei von jeglichem „freundlichen Druck“ fühlen, da durch diese Charta die Neutralität gewahrt bleibt.

Die Dokumentation

Teilnehmerbroschüre/-Liste

In einer Broschüre wird jeder Teilnehmer mit seinem Bild, Namen, Firmenzugehörigkeit und Position im Unternehmen veröffentlicht, in einer Teilnehmerliste die Namen, Firmenzugehörigkeit und Position. Diese Unterlagen werden ausschließlich zu Informationszwecken in Zusammenhang mit den FINAKI-Veranstaltungen genutzt. Alle darüber hinausgehenden Nutzungen sind ausgeschlossen.

Schlussakte

Jeder Teilnehmer erhält von FINAKI nach der Konferenz sein persönliches Exemplar der Schlussakte. Sie enthält folgende Dokumente:

- die Plenarvorträge (soweit vom Redner genehmigt)
- die Dokumentation der Workshopergebnisse
- die Teilnehmerbroschüre

VERANSTALTUNGORT

ANREISE/ABREISE

Veranstaltungsort

München Airport Marriott Hotel
Alois-Steinecker-Straße 20
D-85354 Freising
Tel.: 08161 / 966-0
Fax: 08161 / 966-6255
mhfr.mucfr.ays@marriotthotels.com
www.marriotthotels.com/mucfr

Anreise/Abreise:

Die Reisekosten werden von den Teilnehmern selbst getragen.

Gebühren für die Konferenzteilnahme

Anwenderunternehmen:

Die Gebühr beträgt für jeden Teilnehmer € 1.080,-
zzgl. Mehrwertsteuer.

Anbieterunternehmen:

Die Gebühr beträgt für jeden Teilnehmer € 2.780,-
zzgl. Mehrwertsteuer.

Eingeschlossene Leistungen:

Diese Konferenzgebühren beinhalten auch die Kosten für Unterbringung
und Bewirtung.

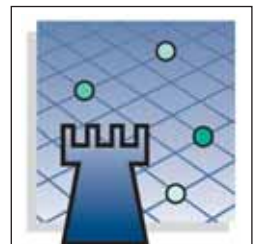
Anmeldung

FINAKI Deutschland GmbH
Managementkongresse
Bahnhofstraße 81
D-82166 Gräfelfing
Tel.: +49 (0) 89/89 82 79 70
Fax: +49 (0) 89/89 82 79 79
info@finaki.de
www.finaki.de



FINAKI Deutschland GmbH
Managementkongresse
Bahnhofstraße 81
D-82166 Gräfelfing

Tel.: +49 (0) 89/89 82 79 70
Fax: +49 (0) 89/89 82 79 79
info@finaki.de
www.finaki.de



seckop
2008