Security, Risiko- & Identity-Management

CONNECT INFORMUNITY

Donnerstag, 1. März 2007
9.00 bis ca. 16.00 Uhr

Palais Eschenbach, Festsaal
Eschenbachgasse 11, 1010 Wien

- **Governance und Compliance**
- **Risikomanagement**
- **Internetkriminalität (Bundeskriminalamt, Computer- & Netzwerkkriminalität)**
- **Marktüberblick Identitymanagement**
- **Stability Management**
- **Neue Trends (IT-Forensik, Mobile, ...)**
- **Security Policy**
- **Standards (ISO 17 799 und ISO 27 001 u. a.)**
- **Best Practices (Raiffeisen Informatik)**

Die Teilnahme ist für IT-Anwender aus Wirtschaft und öffentlicher Verwaltung kostenfrei.
Für IT-Anbieter/-Berater ist eine Gebühr von € 390,– (zuzügl. 20 % MwSt.) zu entrichten.

Referenten: **Roman Brandl** (Sun), **Samuel Brandstätter** (avedos business solutions gmbH), **Theo Christoph** (DATSEC Data Security), **Axel Ciml** (Oxford Computer Group), **Wolfgang Köck** (UPC Austria), **Andreas Kroisenbrunner** (Checkpoint), **Leopold Löschl** (BM für Inneres, BKA – Computer- und Netzwerkkriminalität), **Hannes Passegger** (Telekom Austria), **Peter Rogy** (schoeller network control), **Matthias Schabl** (Novell), **Michaela Weber** (CA), **Günter Weinhandl** (Raiffeisen Informatik)

Moderation: **Peter Fischer** (Berater), **Edmund Lindau** (Computerwelt), **Hans Müller** (Berater), **Otto Zatschek** (Sphinx)

Mit freundlicher Unterstützung von:

avedos · ca · DATSEC DATA SECURITY · inode · Microsoft · Novell · Oxford Computer Group · Raiffeisen Informatik · schoeller · Telekom Austria · Sun microsystems · asf austrian.security.forum · future network

Agenda

8.30 **Registration**

9.00 **Probleme und Erscheinungsformen der Internetkriminalität**
Leopold Löschl (BM für Inneres, BKA – Computer- und Netzwerkkriminalität)

9.40 **IT-Forensik – Ein Blick hinter die Kulissen**
Peter Rogy (schoeller network control)

10.10 **Transparente Rechte-Autorisierung als Sicherheitsfaktor**
Matthias Schabl (Novell)

10.40 **Pause**

11.10 **Secure Identity Management (SIM) bei Raiffeisen**
Günter Weinhandl (R-IT)

11.40 **IT-Risk Management und die Superuser – Vertrauen ist gut, Kontrolle ist Vorschrift!**
Michaela Weber (CA)

12.10 **Identity Management in der Praxis**
Roman Brandl (Sun)

12.40 **Pause**

13.40 **Von der Securitykomponente zum umfassenden Stabilitymanagement**
Hannes Passegger (Telekom Austria)

14.10 **Zwischen Malware-Ausbruch und Sicherheitsupdate**
Theo Christoph (DATSEC Data Security)

14.40 **Identity Lifecycle- and Accessmanagement mit MIIS**
Axel Ciml (Oxford Computer Group)

15.10 **Managed Security vom ISP - professionelles Sicherheitsmanagement für die IT Umgebungen in KMU und Fillialnetzen**
Wolfgang Köck (UPC Austria),
Andreas Kroisenbrunner (Checkpoint)

15.40 **Effizienz in Governance Prozessen durch integriertes Risiko- und Compliance-Management**
Samuel Brandstätter (avedos business solutions gmbH)

16.00 **Ende der Veranstaltung**

Viele neue Begriffe der IT machen eines klar: die IT ist heute in den meisten Unternehmen eng mit dem Geschäftserfolg verbunden. Sicherheit der IT ist kein rein technisches Thema mehr, sie ist ein geschäftrelevanter Aspekt geworden. IT-Entscheidungsträger sind Business Manager. Ausdrücke wie IT-Governance bringen diese Verantwortung klar zur Geltung.

Risk Management und Business Continuity sind Treiber für die Anforderungen an die IT. Das erfolgreiche Umsetzen der Anforderungen erfordert Kenntnisse über die Lösungsmöglichkeiten, von den rechtlichen Rahmenbedingungen über Lösungsstrategien bis zu Produkten und deren Einsatzmöglichkeiten.

Probleme und Erscheinungsformen der Internetkriminalität

Betrugsdelikte, hier vor allem Phishing und Online Shopping, wie die Erfahrungen der letzten Jahre gezeigt haben, sind im Internet stark im ansteigen begriffen. Betroffen kann jeder sein gleichgültig ob Unternehmer oder Privatmann, die Anonymität des »WWW« hilft den Betrügern vielfach leichter an ihre Opfer heran zu kommen.

Das Internet als Tatort für die organisierte Kriminalität – mehr und mehr werden die Vorzüge der grenzenlosen Kommunikation über das Internet auch von Gruppen der organisierten Kriminalität für sich entdeckt. Das Internet bietet sich als Tatort »klassischer« aber auch »neuer« Deliktesformen an.

IT-Forensik – Ein Blick hinter die Kulissen

Peter Rogy
(schoeller network control)

Forensische Analysen und das Wissen, das man dazu benötigt, werden in der heutigen Zeit immer wichtiger, da die Anzahl der Attacken stetig wächst. Auch Wissen darüber, wer gegen ein Unternehmen Hack-Attacken durchführt und mit welchen Techniken dieser agiert, ist wichtig. Aufgebautes Wissen über die Vorgehensweise von »Bösewichten« erleichtert das Verstehen der Angriffsziele und -methoden und die Verteidigung bzw. Abschottung von wichtigen IT-Ressourcen.

Transparente Rechte-Autorisierung als Sicherheitsfaktor

Matthias Schabl
(Novell)

Heutzutage müssen Unternehmen ihre IT-Infrastrukturen nicht nur vor Datendiebstahl schützen und für die Einhaltung gesetzlicher Vorschriften sorgen, sondern auch den Datenschutz von Benutzern gewährleisten. Sicherheits- und Identitätslösungen von Novell unterstützen Sie beim Sichern Ihrer Datenbestände, ohne die betriebliche Effektivität oder neue Geschäftschancen zu beeinträchtigen. Wir helfen Ihnen dabei, die Spreu vom Weizen zu trennen und den richtigen Personen den richtigen Zugriff zu gewähren, ohne dabei Ihr Geschäft zu beeinträchtigen.

Identity Management in der Praxis

Unternehmen sind heutzutage mit noch nie da gewesenen Herausforderungen bei der Sicherung sensibler Daten, der Erhöhung der Effizienz von Geschäftsprozessen und der Kostenkontrolle von Identity Management konfrontiert – und das alles zur selben Zeit. Diese Herausforderungen werden durch ein geschäftliches Umfeld erschwert, in dem Informationssicherheit kritisch ist, Änderungen immer rascher erfolgen und der Druck, gesetzliche Vorschriften einzuhalten, immer größer wird. Unternehmen müssen sich diesen Herausforderungen mit einer Identity-Management-Lösung stellen, die Kosten und Komplexität der sicheren Verwaltung von Zugriffsrechten und Identitätsprofilen reduziert.

Identity Management ist mehr als nur ein zentrales (Meta-)Directory im Unternehmen. Bei der Einführung von Userprovisioning sind alle Aufgaben der davon betroffenen Abteilungen zu beachten und zu integrieren.

Anhand von Beispielen aus der Praxis werden exemplarisch solche Berührungspunkte ausgearbeitet, und das Zusammenspiel mit dem Sun Identity Manager aufgezeigt.

IT-Risk Management und die Superuser – Vertrauen ist gut, Kontrolle ist Vorschrift!

Das Management der IT-Sicherheit in Organisationen hat in den letzten 10 Jahren einen deutlichen Wandel erlebt. Wo zunächst nur eine wachsende Anzahl an technischen Kommunikationsschwachstellen den Einsatz von Firewall und Intrusion Detection notwendig machten, sehen sich IT-Leiter und Geschäftsführer heute mit einer wachsenden Anzahl an Gesetzen und Regularien konfrontiert, die einen Zwang zur Umsetzung konkreter Richtlinien und technischer Maßnahmen implizieren.

Michaela Weber
(CA)

Der Vortrag zeigt, wie auch in heterogenen Umgebungen die Herausforderung einer einheitlichen Policy für verschiedene Betriebsysteme einfach umgesetzt werden kann. Neben einer komfortablen, auf Rollen basierenden Zuteilung von Berechtigungen, wird insbesondere auf die Gewaltentrennung von und eindeutige Zuordenbarkeit bei kritischen Vorgängen eingegangen – denn die Aussagefähigkeit der systemeigenen Logdateien ist begrenzt, wenn der »root« oder »Administrator« Anwender wichtige Daten geändert hat, und die verantwortliche Person unbestimmbar bleibt.

Secure Identity Management (SIM) bei Raiffeisen

Günter Weinhandl
(Raiffeisen Informatik GmbH)

Raiffeisen Informatik GmbH hat als ein Vorreiter in Österreich eine vollständige Lösung zum Thema Secure Identity Management (Identity Management, Single Sign On, PKI mit Smartcard Logon) umgesetzt. Die Lösung ist seit Ende 2005 bei Raiffeisen Informatik und in naher Zukunft im Raiffeisensektor im Einsatz.

Der Vortrag geht auf die Lösung und das

Lösungsportfolio der Raiffeisen Informatik sowie auf die grundlegenden Ansätze einer erfolgreichen Secure Identity Management Einführung ein.

Von der Securitykomponente zum umfassenden Stabilitymanagement

Hannes Passegger (Telekom Austria)

Die Sicherheit und Verfügbarkeit von Unternehmensinformationen ist heute wichtiger als je zuvor. Lücken in der IT-Sicherheit haben nicht selten gravierende wirtschaftliche Verluste sowie Imageschäden zur Folge. Lange Zeit wurde im IT-Sicherheitsumfeld sehr technisch gedacht, und man konzentrierte sich auf einzelne Komponenten wie Firewalls, Virenschutz, Backup-Systeme. IT-Sicherheit sollte aber viel stärker unter einem ganzheitlichen Gesichtspunkt betrachtet werden. Damit steigen zugleich die Anforderungen, weil eine ganzheitliche Betrachtungsweise viele Bereiche vereinigen muss.

Zwischen Malware-Ausbruch und Sicherheitsupdate

Theo Christoph (DATSEC Data Security)

Zero-Day-Exploits sind heutzutage mehr denn je ein Thema. Oftmals ist das Zeitfenster für die Hersteller von Antivirensoftware so gering, dass ein ausreichender Schutz durch Signaturupdates nicht mehr möglich ist. Effizienter Malwareschutz beruht heutzutage auf ausgeprägten, heuristischen Methoden.

Identity Lifecycle- and Accessmanagement mit MIIS

Axel Ciml (Oxford Computer Group)

Microsoft präsentiert den Microsoft Identity Integration Server.

Oxfordcomputergroup, der Parter für MIIS-Lösungen zeigt anhand von Lösungen aus den Bereichen Retail, Insurance und Public Sector Möglichkeiten und Potenziale.

Der Schwerpunkt wird hierbei auf die Integration von AD, SAP, Lotus Notes und RSA gelegt. Weiters wird gezeigt wie die Erweiterungen Reporting, Workflow und die webbasierte Adminoberfläche, alles Eigenentwicklungen von OCG, ihren Beitrag zu SOX leisten können.

Managed Security vom ISP – professionelles Sicherheitsmanagement für die IT-Umgebungen in KMU und Fillialnetzen

Viele Unternehmen wie auch Filialbetriebe sind aufgrund ihrer internen Ressourcen, spezifischen Infrastruktur oder schlichtweg, weil sie sich auf ihr Kerngeschäft konzentrieren wollen, mit dem immer anspruchsvoller werdenden Handling von IT-Security überlastet. Ein Outsourcing an Dritte erscheint manchmal schwierig.

Hier setzt inode Managed Security an: es ist einfach eine Konsequenz des guten Service, dem Kunden neben Internet Access, Kommunikationsdiensten (VoIP/Telefonie) auch komplette Sicherheitslösungen anzubieten. Ein Full Service Konzept von UPC Austria, realisiert mit dem Security Marktführer Checkpoint.

Effizienz in Governance Prozessen durch integriertes Risiko- und Compliance-Management

Samuel Brandstätter (avedos business solutions gmbH)

Der Aufwand, den Unternehmen heute in Compliance-Aktivitäten investieren ist verglichen mit deren Nutzen oft sehr hoch. Der Vortrag stellt eine Methodik zur Ableitung der Compliance aus der unternehmensinternen Risikoanalyse vor. Diese auf einer Scorecard basierende Vorgehensweise erlaubt es, Synergien zwischen den unterschiedlichen Anforderungen aus Risikoanalyse und Compliance zu nutzen und Aufwände zu sparen.

CON•ECT Training Institute:

Voice-over-IP-Security-Workshop

(Sicherheitsrisiken bei IP-Telefonie aufzeigen)

Referent:
Enno Rey
(ERNW Enno Rey Netzwerke GmbH)

Telefonie über das Internet Protocol (Voice over IP, kurz »VoIP«) ist in aller Munde. Sei es die Verlockung »kostenfrei« zu telefonieren, das Einsparungspotential beim Verschmelzen von TK- und IT-Landschaft und -personal oder die Verknüpfung von zahlreichen Messaging-Diensten mit CRM-Programmen u. Ä.: der Phantasie sind (fast) keine Grenzen gesetzt und beflügelt die Vorstellungskraft so mancher Unternehmensführung. Dieser Workshop zeigt Ihnen auf, welche Auswirkungen VoIP auf das Sicherheitsniveau Ihres Netzwerkes hat, wie einfach es ist, VoIP-Telefonate abzuhören/aufzuzeichnen, welche aktuellen Schwachstellen & Angriffe es auf VoIP-Infrastruktur gibt und mit welchen Maßnahmen Sie dem begegnen können.

Workshop-Inhalte

VoIP – Begriffe/Konzepte/Protokoll-Grundlagen

- Protokolle (SIP/H.323/RTP)
- Komponenten (Call-Manager, SIP-Registrar, SIP-Proxy, Media-Gateways)
- Endgeräte (Hardphones, Softphones) Sicherheits-Features und Sicherheits-Lücken von VoIP.
- Angriffe gegen Telefone (etwa Raum-Mithören) und zentrale Komponenten (Call-Manager).
- Mitlesen/Mithören von Telefonaten
- Angriffe gegen Komponenten und Protokolle
- Sicherstellung der Verfügbarkeit.
- Schnittstellen zur klassischen Telefonie.

Sicherheitsmaßnahmen

- Verschlüsselung mit SRTP
- Sicherungsmaßnahmen für SIP
- Trennung von VoIP und Daten mittels Netzwerkdesign (Voice-VLANs, MPLS etc.)
- Herausforderungen an Management und Revision durch VoIP. Checklisten für Audit/Revision

Zielgruppe

Systemadministratoren, Netzwerkadministratoren, Projektleiter, IT-Leiter, IT-Revisoren, Datenschutzbeauftragte, Datensicherheitsbeauftragte

Der Referent:

Enno Rey (CISSP, CISA) ist technischer Geschäftsführer respektive Security Officer der ERNW Enno Rey Netzwerke GmbH (Heidelberg). Neben der formalen Sicherheitsarbeit nach BS7799/ISO17799 sowie der Durchführung vonPenetrations-Tests und Audits großer und mittlerer Netze besteht seine Tätigkeit zur Zeit hauptsächlich aus IT-Security Research.

Termine:	CT060627	**15. Februar 2007**
Ort:	CON•ECT Eventcenter, 1070 Wien	
Gebühr:	€ 750,–	
		Alle Preise zuzüglich 20 % MWSt.

Seminar

Information-Security-Manager

Technologieexperte mit Führungsqualitäten mit Zertifizierungsprüfung nach BS 7799 / ISO 17799

Referenten:
Günther Schreiber (Quality Austria, CIS), **Herfried Geyer** (Siemens Business Services), **Markus Frank** (L-L.M.), **Johann Brunner** (WKO)

Ein Technologie-Experte mit Führungsqualitäten

InformationsSicherheitsManager ist ein Berufsbild mit Zukunft. Mit Ihrer Führungs- und Technologiekompetenz nehmen Sie eine zentrale Position im Unternehmen ein. Sie betreuen die Implementierung und ständige Verbesserung von ISMS und fungieren als Schnittstelle zwischen der obersten Führungsebene und den operativen Bereichen.

Entsprechend weit ist der Bogen der Ausbildungsinhalte gespannt. Der Lehrgang umfasst drei Module, die unabhängig voneinander besucht werden können:

- Die Norm ISO 17799 / BS 7799 (2 Tage)
- Psychologische Grundlagen für IS-Manager (1 Tag)
- Rechtsgrundlagen (1 Tag)

Die Teilnahme an allen drei Seminaren ist Voraussetzung für das Absolvieren der Prüfung. Der erfolgreiche Abschluss wird Ihnen mit dem staatlich anerkannten CIS-Zertifikat bescheinigt, das auch international gültig ist.

- Prüfung IS-Manager (1 Stunde)
- Zertifikat IS-Manager

Modul 1: Die IS-Norm BS 7799 / ISo 17799

Aus Risiko wird messbare Sicherheit

Dieses Zwei-Tages-Modul vermittelt Ihnen das Fundament, auf dem moderne ISM-Systeme aufbauen: die Norm ISO 17799 / BS 7799 mit allen Teilbereichen wie Security Policy, Risk Management oder Business Continuity Planning sowie auch übergeordnete Aspekte wie Organisation oder Prozessmanagement. Mittels praktischer Fallbeispiele wird die selbständige Umsetzung des Gelernten gefördert.

Modul 2: Psychologische Grundlagen für IS-Manager

Soft-Skills: Gewusst wie!

Die Einführung neuer Systeme stößt leicht auf Widerstände – außer man beherrscht die hohe Schule der Psychologie. Dieses eintägige Seminar vermittelt Ihnen die Grundlagen, um das erworbene Fachwissen erfolgreich im Unternehmen umsetzen zu können. Dazu gehören Soft-Skills wie Moderationsfähigkeit, Teamfähigkeit oder Konfliktfähigkeit, aber auch Wissen über Beziehungsmodelle, gruppendynamische Prozesse und Motivationstechniken.

Modul 3: Rechtsgrundlagen für IS-Manager

Gut informiert ist halb gewonnen!

Ein wichtiges Element im Bereich Informationssicherheit sind Gesetze, die den Schutz von Daten regeln. In diesem eintägigen Seminar werden Ihnen vier für Information-Security relevante Schwerpunkte vermittelt: Datenschutz, Wettbewerbsrecht, E-Commerce, Urheberrecht. Mit diesem Überblick verfügen Sie über das grundlegende Rüstzeug, um ein kompetenter Ansprechpartner für zugezogene Rechtsberater zu sein.

Termine:	CB060609	**12. – 15. März 2007**
	CB060610	**21. – 24. Mai 2007**
	CB060611	**18 – 21. September 2007**
	CB060612	**12. – 15. November 2007**
Ort:	Wien	
Gebühr:	**Gesamter Lehrgang IS-Manager** inkl. Prüfung und Zertifikat: € 3.060,–	

Alle Preise zuzüglich 20 % MWSt.

Seminar

Information-Security-Auditor

»oberste Instanz« für Informationssicherheit mit Zertifizierungsprüfung nach BS 7799 / ISO 17799

Referenten:
Günther Schreiber (Quality Austria, CIS)
Peter Soudat (Quality Austria, CIS)

Werden Sie zur »obersten Instanz« für Informationssicherheit

Der Lehrgang zum IS-Auditor ist die ideale Ergänzung für ausgebildete IS-Manager, denn Sie können interne Audits selbst durchführen und Ihre Firma optimal auf externe Audits vorbereiten. Sie sind die »oberste Instanz« für ISMS im Unternehmen, beurteilen das System auf seine Normkonformität hin und zeigen Verbesserungspotenziale auf, bevor ein CIS-Zertifikat verliehen oder verlängert wird.

Der Lehrgang für IS-Auditoren besteht aus einer Einstiegsprüfung und zwei Modulen:

- Technische Einstiegsprüfung (2 Stunden)
- Psychologische Grundlagen (2 Tage)
- Audittechniken (1 Tag)

Um ein hohes Qualifikationsniveau der Auditoren zu gewährleisten, ist ein gültiges IS-Manager-Zertifikat Teilnahmevoraussetzung. Die Ausbildung schließt mit dem staatlich anerkannten CIS-Zertifikat »IS-Auditor« ab und eröffnet vielfältige Berufschancen in einem wachsenden Markt.

- Prüfung IS-Auditor (1 Stunde)
- Zertifikat IS-Auditor

Technische Einstiegsprüfung

IT-Wissen als Fundament

Das Absolvieren der technischen Einstiegsprüfung (Dauer: 2 Stunden) ist eine Voraussetzung für die Teilnahme am IS-Auditorenlehrgang der CIS. Die Prüfungsinhalte werden im Selbststudium erarbeitet und umfassen rund 1 000 Fragen und Antworten, die sich auf technische IT-Grundlagen beziehen (Netzwerke, Betriebssysteme, Datenbanken, Grundsätze der Software-Entwicklung, usw...). Die Prüfung ist nach dem Multiple-Choice-Verfahren schriftlich abzulegen.

Modul 1: Psychologische Grundlagen für IS-Auditoren

Vernetzt denken, erfolgreich handeln

Auditoren sind doppelt herausgefordert: Sie fungieren als Prüfer und als vorausschauende Development-Agents, die Impulse für die Weiterverbesserung des ISM-Systems setzen. Das zweitägige Modul vermittelt soziale Kompetenz, die Fähigkeit, in Systemzusammenhängen zu denken sowie Grundregeln der Kommunikation. Theorie und Praxis ergänzen sich: Der zweite Ausbildungstag umfasst Rollenspiele mit Video-Feedback.

Modul 2: Audittechniken

Fit für die Praxis

Die Durchführung interner und externer Audits ist Inhalt dieses eintägigen Lehrgangsmoduls. Diverse Auditarten für unterschiedliche Typen von Organisationen gehören ebenso dazu wie die einzelnen Arbeitsschritte: Vorbereitung des Audits, Anwendung der Auditfragen, Vorab-Prüfung, Vor-Ort-Audit, Auditanalyse (mit Methoden) und Erstellung des Auditberichts. Wichtig ist auch die Bestimmung von Korrektur- und Verbesserungsmaßnahmen.

Termine:	CB060613	**11. – 13. Juni 2007**
	CB060614	**3. – 5. Dezember 2007**
Ort:	Wien	
Gebühr:	**Gesamter Lehrgang IS-Auditor** inkl. Prüfung und Zertifikat: € 3.060,–	
	Alle Preise zuzüglich 20 % MWSt.	

An
CON•ECT Eventmanagement
Kaiserstraße 14/2
1070 Wien

Tel.: +43 / 1 / 522 36 36 - 36
Fax: +43 / 1 / 522 36 36 - 10
E-Mail: registration@conect.at
http://www.conect.at

Zielgruppe:
Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand, IT-Entscheider, IT-Verantwortliche sowie Vertreter von Medien und Wissenschaft

ANMELDUNG: Nach Erhalt Ihrer Anmeldung senden wir Ihnen eine Anmeldebestätigung. Diese Anmeldebestätigung ist für eine Teilnahme am Event erforderlich.

STORNIERUNG: Falls Sie nach erfolgter Anmeldung doch nicht am Event teilnehmen können, bitten wir Sie, uns unbedingt rechtzeitig Bescheid zu geben, damit wir Ihren Platz an einen anderen Interessenten weitergeben können.

ADRESSÄNDERUNGEN: Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

Anmeldung

CON•ECT EVENTMANAGEMENT

- [x] Ich nehme am Informunity-Event »Security & Identity Management« teil:
- [ ] als IT-Anwender aus Wirtschaft oder öffentlicher Verwaltung **kostenfrei**;
- [ ] als IT-Anbieter/Berater zu **€ 390,–** (+ 20 % MWSt.).

- [ ] Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

Firma:

Titel: | Vorname:

Nachname:

Funktion:

Straße:

PLZ: | Ort:

Telefon: | Fax:

E-Mail:

Datum: | Unterschrift/Firmenstempel:

● Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.

(Bei Nichtzutreffen bitte streichen)

grafik krill
07019