



Gemeinsame Arbeitskonferenz: GI | OCG | BITKOM | SI | TeleTrust



D·A·C·H Security

Technische Universität Darmstadt | 15. und 16. März 2005



Aktuelle Informationen: <http://syssec.uni-klu.ac.at/DACH2005/>

syssec



G D Giesecke & Devrient

secunet



Dienstag • 15. März 2005

08.30 Uhr Registrierung, Kaffee und Tee

09.20 Uhr Begrüßung und Überblick

M. Kreutzer • P. Horster

Sicherheitsinfrastrukturen • Leitung: K.-D. Wolfenstetter

09.35 Uhr PDF-Notariatsdienst für Archive

- Digitale Signatur mit Adobe Acrobat und PDF
- Notariatsdienst
- Validierung und Bestätigung von PDF-Signaturen
- Archivierung signierter PDF-Dokumente
- Langzeitsignatur

G. Jacobson
Secardeo GmbH

10.00 Uhr Einführung von PKI in Großunternehmen – Best Practice

- PKI als Infrastrukturprojekt
- Killerapplikationen
- Kostenverrechnungsmodelle
- Rolloutplanung
- Senior Management Support

R. Martens
TC TrustCenter AG

10.25 Uhr Benutzbarkeitsevaluation von Trustcenter-Software – Windows Server CA

- Benutzbarkeit von Sicherheitsanwendungen
- Verwendetes Framework zur Evaluation von PKI-Software
- Testszenarien für Trustcenter in KMUs
- Funktionsumfang der Windows CA
- Erfahrungsbericht, Beispiele und Ergebnisse

M. Laabs
M. Merz
T. Straub
J. Wunderlich
TU Darmstadt

10.50 Uhr Pause – Zeit für Gedankenaustausch

Single-Sign-On und Authentifikation • Leitung: J. v. Knop

11.20 Uhr Starke Authentifizierung an Employee Self-Services-Kiosksystemen

- Kostensenkung durch Employee Self-Services (ESS)
- ESS-Terminals sorgen für verbesserten Informationsfluss
- Chancengleichheit aller Mitarbeiter im Unternehmen
- Authentifizierung am ESS-Terminal mit RFID-Technologie
- Erhöhte Sicherheit durch Zwei-Faktor-Authentifizierung

G. Schneider
SecurIntegration GmbH

11.45 Uhr Identity Management und Single-Sign-On-Konzepte im WebSphere Portal

- Management von Benutzeridentitäten in heterogenen Systemen
- Single-Sign-On-Konzepte am Beispiel WebSphere Portal
- Browser-basiertes Web-Single-Sign-On
- Backend-Single-Sign-On mit unterschiedlichen Benutzeridentitäten
- Integration mit standardisierten Lösungen der Java Welt (JAAS und JCA)

D. Buehler
T. Hurek
IBM Deutschland GmbH

12.10 Uhr Single-Sign-On im Unternehmen

- Was ist Single-Sign-On (SSO) wirklich?
- Einordnung von SSO im Kontext von Identity- und Access Management
- Klassifikation und Vorstellung der verschiedenen SSO-Systeme
- SSO im Unternehmenseinsatz
- SSO – Quo vadis?

M. Vogel
G. Müller
secunet
Security Networks AG

12.35 Uhr Gemeinsame Mittagspause

Biometrie • Leitung: C. Busch

13.35 Uhr Biometrische Sicherheitslösung – das Projekt ROBIN

- Aufgabenstellung und Ziele des Projektes
- Funktionen des Trust Centers
- Einsatz einer multifunktionalen biometrischen Chipkarte
- Integration der Infrastruktur in Applikationen
- Ausblick und nächste Schritte

G. Scheer
Utimaco Safeware AG
J. de Swart
Landelijk Instituut
Beveiliging Rechter-
lijke Organisatie

Dienstag • 15. März 2005

14.00 Uhr Die virtuelle PIN: Biometrische Verschlüsselung

- Virtuelle PIN
- Biometrie
- Iriserkennung
- Fehlerkorrigierende Codes
- Datenschutz

U. Martini

S. Beinlich

A. Linke

Giesecke & Devrient
GmbH

14.25 Uhr Fusion von biometrischen Verfahren zur Benutzerauthentifikation

- Handschrift als biometrisches Merkmal
- Erkennungsverbesserung durch Fusion
- Merkmalsabstand als Ähnlichkeitsmaß
- Multialgorithmische Systeme
- Testergebnisse

C. Vielhauer

T. Scheidat

Uni Magdeburg

eGovernment und Recht • Leitung: P. Frießem

B

13.35 Uhr Virtuelle Poststelle – Sicherheitsinfrastruktur für eGovernment

- Funktionalitäten der Virtuellen Poststelle
- Sichere Web-, OSCI- und Mail-Kommunikation
- Zentralisierte Zertifikatsvalidierung
- Einsatzszenario am Beispiel DEHSt
- Offene Fragen aus Praxisevaluationen und Lösungsansätze

J. Apitzsch

M. Horstmann

bremen online
services GmbH

A. Schmidt

BSI

14.00 Uhr Identifikationsmodell der Österreichischen Bürgerkarte

- Modell der datenschutzkonformen eindeutigen Identifikation
- Die Bürgerkarte und ihre Schnittstelle (Security Layer)
- Technische Ausprägungen der Bürgerkarte
- Wiederholungsidentitäten
- Identifikation auf Basis ausländischer elektronischer Identitäten

T. Rössler

TU Graz

H. Leitold

A-SIT

14.25 Uhr Rechtliche und technische Entwicklungen qualifizierter Signaturen

- Aktueller Stand der Dinge
- Überblick Benutzer/Kartenprojekte
- Rechtliche Neuerungen durch das 1. SigÄndG
- GKV-Modernisierungsgesetz
- Weitere Anwendungen: JobCard, JKomG, Steuerrecht

J. Klink

Amtsgericht

Kaiserslautern

T. Straub

TU Darmstadt

14.50 Uhr Pause - Zeit für Gedankenaustausch

Sicherheit in Netzen • Leitung: W. Kühnhauser

A

15.20 Uhr Intrusion Detection und Response

- Anforderungen an ein IDS/IRS System
- Funktionsweise und Analysemethoden
- IDS-Architekturen
- Vergleich kommerzieller Systeme mit Open-Source-Ansätzen
- IDS-Testergebnisse: Effizienz der Angriffserkennung

K.-O. Detken

D. Götsche

Decoit GmbH

15.45 Uhr Automatisierte Evaluierung von Firewalls

- Probleme und Risiken komplexer Sicherheitsmechanismen
- Bewertung von Firewallsystemen
- Konzept zur automatisierten Evaluierung von Firewalls
- Anforderungen an eine Testumgebung
- Einsatz in der Praxis

A. Senier

TU Ilmenau

16.10 Uhr Interoperabilität neuer Secure-Messaging-Lösungen

- Mit Absenderauthentifizierung gegen E-Mail Spoofing und Phishing
- Sender Policy Framework und Caller-ID
- Domain Key Verfahren von Yahoo
- E-Mail-Verschlüsselung auf Domain Key Basis
- Interoperabilität etablierter E-Mail-Architekturen

S. Wappler

noventum consulting
GmbH



Dienstag • 15. März 2005

- 16.35 Uhr Konfigurierbare Sicherheitsmaßnahmen für WebServices mit Apache AXIS** **J. Key**
D. Fischer
NetSys.IT GbR
- Probleme bei der Sicherung von WebServices
 - Interoperabilität im Kontext von WebServices und WebService Security
 - Entwurf eines Framework zur Absicherung von WebServices
 - Verwendung von XML-Signature und XML-Encryption
 - Demonstration des Entwicklungsstandes des Framework

BMW-Leitprojekt VERNET • Leitung: K. Rosmus

B

- 15.20 Uhr Beweiskräftige Archivierung elektronisch signierter Dokumente** **P. Schmücker**
FH Mannheim
- Beweiswerterhalt mit qualifizierten elektronischen Signaturen
 - Verifikationsdatenbeschaffung und automatische Signaturerneuerung
 - Rechtssichere Transformation von Dokumenten
 - Rechts-Simulationsstudie
 - Standardisierungsinitiative zur Signaturerneuerung
- 15.45 Uhr SELMA – Sicherer elektronischer Messdatenaustausch** **N. Zisky**
PTB Berlin
- Signaturen und Zertifikate
 - Sicherheit in Anwendungen
 - Architekturen
 - Verbraucherschutz
 - Konfigurierbare Sicherheit
- 16.10 Uhr Mikro-SINA – Hands-on-Experiences with the Nizza Security Architecture** **C. Helmuth**
A. Warg
N. Feske
TU Dresden
- Komplexität von Betriebssystemen als Sicherheitsproblem
 - Minimale vertrauenswürdige Plattform (TCB)
 - Mikrokern-basierte Sicherheitsarchitektur Nizza
 - Wiederverwendung bestehender Software bei höherer Sicherheit
 - Hochsicheres VPN als Anwendungsszenario
- 16.35 Uhr Model Driven Security** **D. Basin, J. Doser**
ETH Zürich
B. Hollunder
T. Lodderstedt
Interactive Objects
Software GmbH
- Model Driven Architecture (MDA)
 - Role-based Access Control (RBAC)
 - J2EE Security
 - NET Security
 - Modeling Security Policies
- 17.00 Uhr Ende erster Konferenztag**
- 19.30 Uhr Gemeinsames Abendessen**

Programmkomitee

- | | | |
|--|---------------------------------------|--|
| P. Horster • Uni Klagenfurt (Vorsitz) | P. Kraaibeek • secunet | A. Roßnagel • Uni GH Kassel |
| H. Baier • FH Bingen | W. Kühnhauser • TU Ilmenau | P. Schartner • Uni Klagenfurt |
| J. Bizer • ULD Schleswig-Holstein | P.J. Kunz • DaimlerChrysler | I. Schaumüller • ITSB Linz |
| C. Busch • Fraunhofer IGD | S. Lechner • Siemens | R. Steinmetz • TU Darmstadt |
| J. Dittmann • Uni Magdeburg | I. Münch • BSI | J. Taeger • Uni Oldenburg |
| C. Eckert • TU Darmstadt | C. Paar • Uni Bochum | S. Teiwes • Ernst & Young CH |
| W. Effing • Giesecke & Devrient | S. Paulus • SAP | S. Teufel • Uni Fribourg |
| B. Esslinger • Deutsche Bank | G. Pernul • Uni Regensburg | C. Tschudin • Uni Basel |
| T. Faber • secure-it.nrw.2005 | N. Pohlmann • FH Gelsenkirchen | J. von Knop • Uni Düsseldorf |
| D. Fox • Secorvo | R. Posch • TU Graz | G. Weck • Infodas |
| P. Frießem • Fraunhofer SIT | H. Reimer • TeleTrust | M. Welsch • IBM D |
| S. Janisch • Uni Salzburg | K. Rosmus • IABG | K.-D. Wolfenstetter • T-Systems |
| D. Jäpel • IBM CH | | |

Organisation

P. Kraaibeek secunet • **D. Cechak** Uni Klagenfurt • **C. Eckert** TU Darmstadt • **D. Lührs** DZI Darmstadt

Mittwoch • 16. März 2005

Konzepte und Anwendungen • Leitung: H. Reimer

09.00 Uhr Tele-Lab IT-Security – IT Sicherheitstraining im Internet

- Sicherheitsausbildung mittels „real-life“ Übungen im Tele-Lab-System
- Vorteile gegenüber bisherigen Schulungsmethoden
- Tele-Lab als CD- und Internetversion
- Architektur und Nutzung der Internet-basierten Version
- Einsatzmöglichkeiten und zukünftige Entwicklungen

D. Cordel

Ji Hu

C. Meinel

Hasso-Plattner-Institut

09.25 Uhr Sicherheitsmodelle für computergestützte Teamarbeit

- Anforderungen an Sicherheitsmodelle für Workflow-basierte Teamarbeit
- Analyse existierender Systeme
- Motivation für einen ganzheitlichen Modellansatz
- Vorstellung eines Integrationsmodells
- Anwendung des Modells anhand eines Praxisbeispiels

W. Kühnhauser

G. Welsche

TU Ilmenau

09.50 Uhr Automatisierte Recherche von Markenpiraterie im Internet

- Internet als wichtiges Medium beim Aufbau von Marken
- Schutz vor Markenpiraterie als neue Herausforderung
- Missbrauch von Logos, Markennamen und Produktabbildungen
- Automatisierte semantische Analyse von Webinhalten
- Effektives Werkzeug für Produktdetektive

P. Ebinger

U. Pinsdorf

Fraunhofer IGD

10.15 Uhr Vertrauliche Videoüberwachung mit geeigneter Zugriffsstruktur

- Systemarchitektur
- Privacy-Aspekte
- 4-Augen-Prinzip
- Zugriffskontrolle
- Verteilte Entschlüsselung

F. Kollmann

M. Schaffer

P. Schartner

Uni Klagenfurt

10.40 Uhr Pause – Zeit für Gedankenaustausch

Signaturen und Anwendungen • Leitung: W. Effing

11.10 Uhr eBilling mit digitaler Signatur im ASP-Verfahren

- Versand elektronischer Rechnungen – Ökonomische Relevanz
- Gesetzliche und steuerliche Anforderungen
- eBilling und ASP – Der schnelle Einstieg in die qualifizierte Signatur
- Betrachtung der technischen Integration
- eBilling im Kontext der IT-Security

C. Rybak

LogAgency GmbH

11.35 Uhr Elektronisch signieren mit eigenhändiger Unterschrift

- TabletPC als Erfassungsgerät
- Sicherheitsmerkmale bei Aufnahme und Vergleich
- Prozess-Reorganisation
- Anwendungsbeispiele
- Nutzererfahrungen & Usability

T. Kleemann

Klinikum Ingolstadt

J. M. Lenz

C. Kaplan

Softpro GmbH

& Co. KG

12.00 Uhr Einsatz von Zertifikaten in einem mittelständischen Unternehmen

- Zertifikatsverwaltung integriert in typischer Büroumgebung
- Open Source als Grundlage für die Realisierung
- Teilnehmen ohne Investitions- und Kostenhürden
- Rechteverwaltung als Ergänzung zur Authentifikation
- Offen für den elektronischen Heilberufeausweis

H. Musielak

R. Winkelmann

Kassenzahnärztliche

Vereinigung Baden-

Württemberg

Elektronische Geschäftsprozesse • Leitung: I. Münch

11.10 Uhr Sicheres Web Shopping

- Potentielle Angreifer
- Ziele der Angriffe
- Sicherheit von Open Source vs. Closed Source
- Interaktion zwischen Systemkomponenten
- Angriffe auf Web Shops

K. Knorr

H. Stormer

Uni Fribourg



Mittwoch • 16. März 2005

11.35 Uhr Kundenbindung durch ein anonymes Rabattsystem

- Kundenbindung im elektronischen Handel
- Kundenbindungsprogramme und Rabattsysteme
- Anreiz zum Kauf durch Treuepunkte
- Ausgleich von Händler- und Kundeninteressen
- Anonymes, zählerbasiertes, elektronisches Rabattsystem

C. Eckert
M. Enzmann
S. Okunick
M. Schneider
Fraunhofer SIT

12.00 Uhr Schutzprofilentwicklung für Internethandel mit mobilen Endgeräten

- Sinn und Zweck eines Schutzprofils
- Sicherheitsrisiken bei Internetauktionen
- Schutzprofil und Systementwicklung
- Mobile Aspekte im entwickelten Schutzprofil
- Ein prototypisches Auktionssystem

M. Haisch
E. Kujaw
Fraunhofer SIT

12.25 Uhr Gemeinsame Mittagspause

Aspekte mobiler Sicherheit • Leitung: S. Lechner

13.25 Uhr Mobile Endgeräte im Unternehmen – Risiken und Schutzmechanismen

- Besonderheiten mobiler Endgeräte im Bezug auf IT-Sicherheit
- Mobile Geräte und sensible Daten
- Mobile Geräte als Hintertür ins Unternehmensnetz
- Wireless Security
- Übersicht über Produktbereiche und Lösungsansätze

S. Strobel
cirosec GmbH

13.50 Uhr Kryptographische Algorithmen für Low-cost-RFID-Systeme

- Low-cost-RFIDs: Technologie und Anwendungsfelder
- Applikationsabhängige Algorithmenauswahl
- Angriffsziele, Angriffsszenarien und Risikoabschätzung
- Sicherheit und Kenngrößen ausgewählter kryptographischer Algorithmen
- Fallbeispiele

W. Schindler
et al.
BSI

14.15 Uhr Erstellung sicherer Anwendungen auf (U)SIM-Karten

- Die (U)SIM-Karte als Plattform für sichere Anwendungen
- Stärken und Grenzen der verschiedenen Anwendungstypen
- Sicherheitsmechanismen zum Schutz von Anwendungen
- Toolgestütztes Entwickeln und Testen von Anwendungen
- Beispiele für sichere (U)SIM-Kartenanwendungen

M. Horak
W. Rankl
Giesecke & Devrient
GmbH

14.40 Uhr Pause – Zeit für Gedankenaustausch

Perspektiven • Leitung: N. Pohlmann

15.10 Uhr Einsatz von IPv6 zur Gewährleistung von Sicherheit beim Smarter Wohnen

- IT-gestützte Mehrwertdienste
- Dienstleistungsplattform: Anforderungen und Hintergrund
- Verständnis von Sicherheit im Anwendungsgebiet Smarter Wohnen
- Migration von Sicherheitskomponenten
- Sicherheitsaspekte von IPSec und Mobile IP

J. Meis
L. Schöpe
Fraunhofer ISST

15.35 Uhr Digitale Fingerabdrücke in Video-on-demand-Szenarien

- Try & Buy Geschäftsmodell im Video-on-demand-Bereich
- Sicherheit durch digitale Fingerabdrücke
- Identifizierung des Kunden
- Schutz vor illegalen Kopien
- Beispielszenarien – DivX und DVD

E. Hauer
M. Steinebach
Fraunhofer IPSI

16.00 Uhr Sicherheitsanwendungen auf Basis intelligenter Speicherpolymere

- Optische Datenspeicherung in Polymeren
- Holographische Hardware-Verschlüsselung
- Speicherung großer Mengen vertraulicher und sensibler Informationen
- Ausweise für multiple biometrische Merkmale
- Hochsicheres Zugangskontrollsystem: Angriffe und Schutzmechanismen

T. Hupe
S. Völkening
H. Jüngermann
Bayer Innovation
GmbH

16.25 Uhr Konferenzende

... als Referenten haben sich zusätzlich zur Verfügung gestellt:

Einsatzgebiete nicht-blinder Wasserzeichen

- Unterscheidung blinder und nicht-blinder Wasserzeichenverfahren
- Vorteile beim Auslesen der Wasserzeichen aufgrund vorhandener Originale
- Identifizieren des Originals
- Methoden zur Unterstützung nicht-blinder Ansätze
- Beispielanwendungen

M. Steinebach
L. Croce Ferri
Fraunhofer IPSI

Designing XML Security Services for Biodiversity Networks

- Erweiterung eines Biodiversitätsnetzwerks um Sicherheitsdienste
- Akzeptanzerhöhung durch Analyse der Anwenderanforderungen
- Design von XML-basierten Sicherheitsdiensten
- Identitäts- und Rechtemanagement mit XACML und SAML
- Perspektive: Absicherung von XML-Dokumenten

R. Tolksdorf
L. Suhrbier
E. Langer
Freie Universität
Berlin

Risikoeinschätzung nach BS PAS 56 und Sarbanes-Oxley

- Neue Vorgaben in der IT-Sicherheit
- Internes Kontrollsystem der Unternehmen
- BS PAS 56, Sarbanes-Oxley, ISO 17799 neu
- Kriterien für Bewertung und Überprüfung
- Corporate Governance

R. von Rössing
KPMG

PKI in der Datenschutzpraxis

- Symbiose IT-Sicherheit – praktizierter Datenschutz
- Datenschutz und PKI: Synergieeffekte zwischen BDSG und SigG
- Qualitätsmerkmale hochwertiger digitaler Signaturen
- PKI-Lösungen als ökonomischer Erfolgsfaktor
- Die Keyfacts der Zukunft für Datenschutz und PKI im Unternehmen

K. Blossey
C. Weber
Verimax GmbH

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz

Partner der Konferenz:



Giesecke & Devrient

Giesecke & Devrient (G&D) ist Technologieführer bei Smart Cards und Anbieter chipkartenbasierter Lösungen für die Bereiche Telekommunikation, elektronischer Zahlungsverkehr, Gesundheit, Identifizierung, Transport sowie Internet-Sicherheit (PKI). G&D ist zudem führend in der Herstellung von Banknoten und Sicherheitsdokumenten sowie in der Banknotenbearbeitung. Die G&D Gruppe mit Sitz in München hat Tochterunternehmen und Joint Ventures in der ganzen Welt. Im Geschäftsjahr 2003 beschäftigte das Unternehmen rund 6.800 Mitarbeiter und erwirtschaftete einen Umsatz von 1,05 Milliarden Euro. www.gi-de.com



secunet Security Networks AG. secunet ist einer der führenden europäischen Anbieter von Produkten und Beratungsleistungen auf dem Gebiet hochkomplexer IT-Sicherheitssysteme.

Das Unternehmen stellt mit über 200 Mitarbeitern die komplette Leistungsbandbreite der IT Security zur Verfügung. Kunden erhalten Beratung, Entwicklung und Integration sowie Schulung und Service aus einer Hand. www.secunet.com



secure-it.nrw.2005. Die Landesinitiative für mehr Sicherheit und Vertrauen in elektronische Geschäftsprozesse hat das Ziel, innovative Geschäftsprozesse auszubauen und zu fördern. Die Aktivitäten umfassen die Förderung der IT-Sicherheit und der Akzeptanz elektronischer Geschäftsprozesse unter Erschließung innovativer Wachstumsfelder. www.secure-it.nrw.de



syssec. Neben Kernkompetenzen in den Bereichen Sicherheitsinfrastrukturen und Angewandte Kryptologie verfügt die Forschungsgruppe Systemsicherheit – syssec – über Erfahrungen beim Aufbau komplexer sicherheitsrelevanter Systeme in unterschiedlichen Anwendungsfeldern, etwa im Kontext elektronischer Passsysteme, tokenbasierter Sportereignisse und bei Sicherheitssystemen für Automobile. Von besonderer Relevanz sind dabei der Einsatz von Chipkarten und weiterer Sicherheitstoken sowie ein bedarfsgerechtes Schlüsselmanagement. Zudem steht die Forschungsgruppe syssec als unabhängiger wissenschaftlicher Projektbegleiter und Berater für sicherheitsrelevante Projekte, auch im Konfliktfall (z.B. bei Patentverletzungen oder der Auslegung von Pflichtenheften) zur Verfügung. Durch unser grenzüberschreitendes Netzwerk zu zahlreichen universitären und industriellen Forschungseinrichtungen und zur relevanten Industrie können wir gemeinsam komplexe Probleme – auch interdisziplinär – behandeln. *Kontakt: syssec@uni-klu.ac.at*



Anmeldung & Teilnahmebedingungen

D•A•CH Security 2005

15. und 16. März 2005

Technische Universität Darmstadt



via Fax an: ++49 (0)5921-722-493

oder Online-Formular unter: <http://syssec.uni-klu.ac.at/DACH2005/html/anmeldung.html> oder an:

Organisationskomitee D•A•CH Security 2005

Peter Kraaibeek

Bogenstr. 5a

D-48529 Nordhorn

Telefon: ++49 (0)5921-722-490

E-Mail: Peter@Kraaibeek.com

Anmeldung zur Konferenz

.....
Name

.....
Firma

.....
Funktion

.....
Straße

.....
PLZ/Ort

.....
Tel.-Nr.

.....
Fax-Nr.

.....
E-Mail

- Hiermit melde ich mich verbindlich zur Arbeitskonferenz
D•A•CH Security 2005 am 15. und 16. März 2005 an der Technischen
Universität Darmstadt an.
- Ich kann an der Tagung nicht teilnehmen, bestelle aber ein Exemplar
des Tagungsbandes zum Preis von € 59.– inkl. MWSt.



Teilnahmebedingungen

Bei Anmeldung bis zum 15. Februar 2005 beträgt die Frühmeldegebühr € 285.– zzgl. MWSt. (330,60 €), anschließend beträgt die Teilnahmegebühr € 330.– zzgl. MWSt. (382,80 €).

Die Teilnahmegebühr beinhaltet ein Exemplar des Tagungsbandes (Hardcover mit ISBN), Pausengetränke, Mittagessen an beiden Konferenztagen und ein gemeinsames Abendessen am ersten Konferenztag.

Bei Stornierung der Anmeldung bis 8. März 2005 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75.– (inkl. MWSt.) erhoben. Nach dem 8. März 2005 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Die Teilnahmegebühr überweise ich sofort nach Erhalt der Anmeldebestätigung und Rechnung unter Angabe der Rechnungsnummer auf das Tagungskonto.

.....
Ort und Datum

.....
Unterschrift