



## Montag, 08.05.06 Tutorien

Alle Tutorien finden parallel statt und starten um 10:00 Uhr und enden gegen 17:30 Uhr.  
Bitte kreuzen Sie Ihr bevorzugtes Tutorium an.

**Tutorium 1: Aktuelle Themen der IT-Security**  
Angriffe, Konzepte, Lösungen im Überblick  
(mit Live-Demo)

- Vorstellung realer Angriffsszenarien
- Grundlagen der IT-Sicherheit
  - Umgang mit Risiken, Schutzziele, Elementare Maßnahmen
  - Security Policy, Grundschutz, BS 7799
- Grundlagen der Verschlüsselungstechnologie
- Einführung, Kryptografie, aktuelle Standards
- Lösungen zur E-Mail Sicherheit
  - Client-Plug-Ins, Gatewaylösungen
- Von Firewall bis VPN
  - Konzepte, DMZ, Betrieb, Praxis
- Sicherheitsfunktionen von Windows 2003/XP
  - Distributed Security Services, SmartCards
- Sichere Server
  - Logging, Backup, Hardening

Hans-Joachim Knobloch,  
Secorvo Security Consulting GmbH

**Tutorium 2: VoIP-Security**  
Technische und Rechtliche Sicherheit  
(mit Live-Demo von Angriffen)

- Kurzvorstellung VoIP
- Gefahren bei der Nutzung von VoIP
  - Angriffe gegen VoIP-Kommunikation
  - Bedrohungen durch Verwendung dynamischer Ports
  - Transport von Malware über VoIP-Protokolle
- Angriffe auf Handy- und WLAN-Funkstrecken
- Rechtliche Sicherheit bei VoIP
  - Fermeldegeheimnis und Betriebsverfassungsrecht
- Sicherheitsanforderungen an VoIP

Ulrich Emmert, Frank Gebert  
esb Rechtsanwälte

**Tutorium 3: Layer-2 Security**  
Angriffe gegen die Netzwerk-Infrastruktur  
(mit Live-Demo von Angriffen und Tools)

- Überblick zu Layer-2 Technologien und Protokollen
- Vorstellung der wichtigsten Sicherheitsprobleme
- Layer-2 Security Features (Private VLANs, DHCP Snooping, ARP Inspection, 802.1X)
- Ausblick auf moderne WAN-Technologien (Metro Ethernet, Ethernet over MPLS, Virtual Private LAN Services)
- Auswirkungen auf die Layer-2 Security

Enno Rey  
ERNW Netzwerke GmbH

11:30 - 12:00 Uhr Kaffeepause  
13:00 - 14:30 Uhr Mittagspause  
16:00 - 16:30 Uhr Kaffeepause

## Dienstag, 09.05.06

**10:00 Uhr – 10:15 Uhr**  
Begrüßung/Übersicht

Detlef Weidenhammer,  
GAI NetConsult GmbH

**10:15 Uhr – 11:00 Uhr**  
Sicherer Umgang mit modernen Kommunikationsformen

- Instant Messaging: Von ICQ bis Jabber - Nutzen oder verbieten?
- Peer-to-Peer: von eDonkey bis BitTorrent - was geht davon im Unternehmen?
- Anonymisierungsdienste im Unternehmen: Datenschutz gegen IT-Sicherheit?
- Von http-Tunnel bis JAP: Warum überhaupt noch eine Firewall?

Prof. Dr. Rainer W. Gerling  
Max-Planck-Gesellschaft

**11:00 Uhr – 11:45 Uhr**  
Zunehmende Kriminalisierung des Internet

- Massenhaft vorgetragene Angriffe (Phishing, Botnets usw.)
- Gezielte Angriffe mit Spyware
- Angriffe auf kritische Infrastrukturen
- Abwehrmaßnahmen

Detlef Weidenhammer,  
GAI NetConsult GmbH

**12:15 Uhr – 13:00 Uhr**  
IT-Sicherheit in kritischen Infrastrukturen

- Einführung in die Thematik „Kritische Infrastrukturen“
- Nationale und internationale Aktivitäten
- KRITIS-Materialien des BSI
- Sicherheitsrichtlinie und -check in der Praxis

Stefan Gunzelmann,  
consequa GmbH

**14:30 Uhr – 15:15 Uhr**  
Sicherheitszonen in der LAN-Infrastruktur

- Seiteneffekte konvergenter Netze auf die Sicherheit
- Sicherheitsinfrastrukturen bei Gefährdungen von innen
- Firewalls und Protokolle in verteilten Systemen
- Authentifizierung und Autorisierung am LAN-Zugang: Techniken und ihre Grenzen
- Zugang für Gäste und Fremdfirmenmitarbeiter

Dr. Simon Hoff,  
ComConsult Beratung und Planung GmbH

**15:15 Uhr – 16:00 Uhr**  
Entwicklung eines Konzepts für Security Incident Handling

- Einbettung des Security Incident Handlings in die vorhandenen Prozesse (Sicherheitsprozess, Business Continuity, Disaster Recovery)
- Komponenten des Security Incident Handlings und Berücksichtigung der verschiedenen Bedrohungsphasen

•Definition eines Security Incident Handling Prozesses

•Erfahrungen bei der Umsetzung

Sven Schumann,  
HUK-Coburg-Allgemeine Versicherung AG

**16:30 Uhr – 17:15 Uhr**  
Business Continuity Planning in der IT-Praxis

- Einführung in die BCP-Thematik
- Einsatz eines Scoring-Verfahrens bei der Bestimmung kritischer Prozesse
- Notfallpläne und ihre Praxistauglichkeit
- Test, Pflege und Revision der Planung

Holm Diening,  
GAI NetConsult GmbH

**17:15 - 18:00 Uhr**  
Security Awareness - Mitarbeitersensibilisierung

- Mitarbeiter als „letzte Bastion“ der IT-Sicherheit
- Das 4-Phasen-Konzept einer Awareness-Kampagne
- Zentrale Erfolgsfaktoren
- Praxisbeispiele

Dirk Fox,  
Secorvo Security Consulting GmbH

11:45 - 12:15 Uhr Kaffeepause  
13:00 - 14:30 Uhr Mittagspause  
16:00 - 16:30 Uhr Kaffeepause  
ab 18:30 Uhr Happy Hour

## Mittwoch, 10.05.06 Praxis-Workshops - Die Durchführung der Workshops wird am Teilnehmerinteresse ausgerichtet.

**9:00 Uhr – 12:30 Uhr**

**Workshop 1:**  
Einsatz von netzwerk-basierten IPS

**Workshop 2:** Modern Hacking - Know your Enemy  
Live-Demo von Angriffstechniken

**Workshop 3:** Business Continuity Planing im IT-Umfeld  
Live-Demo eines Tools

**Workshop 4:** Sicherheit von BlackBerry und Alternativlösungen - Vergleich unterschiedlicher Lösungen

**14:00 Uhr – 17:30 Uhr**

**Workshop 5:** IT-Security Best Practice  
Top-10 Tips und Tricks in der Diskussion

**Workshop 6:**  
Intelligente Analyse von Security Log Files

**Workshop 7:** User Identity based access control-  
Zugriffsschutz auf allen Ebenen

**Workshop 3:** Business Continuity Planing im IT-Umfeld  
Live-Demo eines Tools

Bitte wählen Sie zwei der aufgeführten Workshops auf der Folgeseite aus. Detaillierte Inhalte der aufgeführten Workshops finden Sie auf der Folgeseite.

11:00 - 11:30 Uhr Kaffeepause  
12:30 - 14:00 Uhr Mittagspause  
16:00 - 16:30 Uhr Kaffeepause

## Donnerstag, 11.05.06

**9:00 Uhr – 10:00 Uhr**  
Projektbericht: IT-Sicherheit nach BS 7799

- Ziel: Beratung zu organisatorischen und strategischen IT-Sicherheitsmaßnahmen
- Anwendung von ISO-Standard 17799 und BS 7799-2
- Pflichtenheft, IT-Assessment, Risikoanalyse
- Erstellung von Security Policy, Notfallkonzept und Sicherheitshandbuch

Frank Spanier,  
DKV Euro Service GmbH & Co KG,  
Stefan Schänzer,  
BDG GmbH & Co KG

**10:00 Uhr – 11:00 Uhr**  
Prozessorientiertes IT-Sicherheitsmanagement mit ITIL

- ITIL: die Vorstellung
- Der Prozess ITIL Security Management
- Maßnahmen und Implementierung
- Koexistenz mit ITSM-Standards

Christian Aust,  
.consecco

**11:30 Uhr – 12:30 Uhr**  
Projektbericht: Aufbau eines sicheren Extranet-Webportals

- Projektstart: Business vs. Security Requirements
- Durchführung einer Risikoanalyse
- Aufbau einer Schutzlösung mit Web Application Firewall und Access Management
- Aufbau der zugehörigen Sicherheitsorganisation

Martin Noll,  
Schering AG

**13:45 Uhr – 14:45 Uhr**  
Evaluierung von Web Application Firewalls

- Evaluierungskriterien des Web Application Security Consortiums
- Überblick zu den am Markt verfügbaren Produkten
- Bewertung und KO-Kriterien in einzelnen Szenarien
- Hinweise für die eigene Produktauswahl

Frank Breitschaft,  
GAI NetConsult GmbH

**14:45 Uhr – 15:45 Uhr**  
Sicherheit für service-orientierte Architekturen (SOA)

- SOA - ein Überblick
- Technische Grundlagen: XML Web Services, Architekturprinzipien
- Umsetzung von SOA-Sicherheit
- Vorstellung eines Fallbeispiels

Sebastian Staamann,  
PrismTech GmbH

**15:45 Uhr**  
Zusammenfassung und Schlusswort

Detlef Weidenhammer,  
GAI NetConsult GmbH

11:00 - 11:30 Uhr Kaffeepause  
12:30 - 13:45 Uhr Mittagspause  
16:00 Uhr Ende der Veranstaltung



# Faxantwort an 030/417898-300

## Name \_\_\_\_\_

## Bitte treffen Sie hier Ihre Wahl

Praxis-Workshops: Bitte kreuzen Sie zwei Workshops an (einen vormittags, einen nachmittags)

9:00 - 12:30 Uhr

### 1 Workshop 1: Einsatz von netzwerk-basierten IPS

- IPS versus IDS und Abgrenzung zu Firewalls: Motivation für IPS
- Funktionsweise von IPS: Techniken zur Erkennung von Angriffen
- Aufbaukonzepte, Redundanz und Performance
- Zu beachtende Aspekte bei der Auswahl von IPS
- Produktbeispiele
- Praktische Erfahrungen

Dr. Simon Hoff,  
ComConsult Beratung und Planung GmbH

### 2 Workshop 2: Modern Hacking - Know your Enemy Live-Demo von Angriffstechniken

- Schwachstellentrends 2005 / 2006
- Passive Zielfindung per Suchmaschine (Google-Hacking und Co.)
- Moderne Exploittechniken und -frameworks
- Angriffe auf Applikationsebene
- Rootkits und Anti-Forensics

Björn Fröbe,  
GAI NetConsult GmbH

### 3<sub>v</sub> Workshop 3: Business Continuity Planing im IT-Umfeld Live-Demo eines Tools

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege
- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

Holm Diening,  
GAI NetConsult GmbH

### 4 Workshop 4: Sicherheit von BlackBerry und Alternativlösungen Vergleich unterschiedlicher Lösungen

- Einführung und Überblick zu den im Workshop vertretenen Produkten
- Sicherheitsaspekte einer Mobile PIM-Lösung:
  - Schutz der Endgeräte
  - Schutz der Kommunikation
  - Schutz der zentralen Server
- Zentrales Management und Überwachung
- Live-Demonstrationen der verschiedenen Lösungen
- Auswahlkriterien für die eigene Produktauswahl

Frank Breitschaft,  
GAI NetConsult GmbH

14:00 - 17:30 Uhr

### 5 Workshop 5: IT-Security Best Practice Top-10 Tips und Tricks in der Diskussion

- Vorgesehene Themen sind:
- Konfiguration von Webbrowsern
  - Sicherung von Webservern
  - Sichere E-Mail
  - Aufbau einer sicheren Adminumgebung
  - VPN (IPsec und SSL)
  - Secure RAS

Björn Fröbe, Dr. Torsten Johr,  
GAI NetConsult GmbH,  
Dr. Simon Hoff, Andreas Meder,  
ComConsult Beratung und Planung GmbH,

### 6 Workshop 6: Intelligente Analyse von Security Log Files

- Security Log File Korrelation mit Aufzeichnung und Rekonstruktion kritischer Ereignisse
- Welche Art der Event-Korrelation macht Sinn?
- Anforderungen an einen Tool-Einsatz
- Vorgehensweise bei der Suche nach „Critical Events“
- Ergänzung forensischer Untersuchungen
- Nutzung der Erkenntnisse auch für Basel II, Sarbanes-Oxley etc.
- Praktische Beispiele und Hands-On

Paul Hoffmann,  
DATAKOM GmbH,  
Peter Weinlich,  
GTEN AG

### 7 Workshop 7: User Identity based access control- Zugriffsschutz auf allen Ebenen Live-Demos unterschiedlicher Technologien

- Einführung: Authentisierung und Authorisierung - Wer bin ich und was darf ich
- Authentisierung und Authorisierung gestern, heute und morgen
- Zugriffssicherung - Protokolle und Methodik im Überblick NAP, NAC, 802.1x in der Praxis
- Identity based access control: Grenzen ziehen, wie und wo
- Betrachtung rechtlicher Aspekte

Carsten Poppe,  
entrada Kommunikations GmbH

### 3<sub>N</sub> Workshop 3: Business Continuity Planing im IT-Umfeld Live-Demo eines Tools

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege
- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

Holm Diening,  
GAI NetConsult GmbH