Sicherheits- & Identitymanagement

IT und Recht und Standards

CONNECT INFORMUNITY

Donnerstag, 21. Februar 2008
9.00 – 16.00 Uhr

Industriellenvereinigung Österreich,
Urban-Saal
1031 Wien, Schwarzenbergplatz 4

- **Gesetze und Verordnungen zu Security aus der Sicht der Revision**
- **Digitale Signatur & IT und Recht**
- **ISO 27 001 – Standards und Zertifizierung**
- **Sicherheits & Identitymanagement**
- **Web Security**
- **Best Practice des Bundesrechenzentrum zu Sicherheitsarchitektur**
- **Best Practice der Raiffeisen Informatik zu Sicherheits & Identitymanagement**

Mit begleitendem Seminarprogramm!

Kostenfreie Teilnahme für IT-Anwender.

Für IT-Anbieter und Berater fällt eine Gebühr in Höhe von € 390,– exkl. MwSt. an.

Referenten:

Dr. Christoph Brenn (angefragt), **Jimmy Heschl** (KPMG / ISACA), **Robert Jamnik** (CIS-Zertifizierungsauditor), **Rudolf Kochesser** (Telekom Austria), **Johannes Mariel** (Bundesrechenzentrum GmbH), **Krzysztof Müller** (Telekom Austria), **Andrea Nowak** (Austrian Research Centers GmbH – ARC), **Lucas Pachler** (Raiffeisen Informatik GmbH), **Helmut Taumberger** (Fujitsu Siemens), **Peter Weierich** (Völcker Informatik AG)

Mit freundlicher Unterstützung von:

asf austrian.security.forum

SECURITY CIS CERTIFICATION INFORMATION

FUJITSU COMPUTERS SIEMENS

RAIFFEISEN INFORMATIK

TELE KOM AUS TRIA

ISACA Serving IT Governance Professionals Austria Chapter

future network

Agenda

Preliminary Program, Änderungen vorbehalten!

8.30 **Registration**

9.00 **Einfluss von Gesetzen und Verordungen auf IT-Revision und -Security**
Jimmy Heschl (KPMG / ISACA)

9.30 **Identity Management als Schlüssel zur IT-Governance**
Peter Weierich (Völcker Informatik AG)
Helmut Taumberger (Fujitsu Siemens)

10.00 **Secure Identity Management – soviel Sicherheit muss sein!**
Lucas Pachler (Raiffeisen Informatik GmbH)

10.30 **Pause**

11.00 **IT in Balance – Bedeutung von Risikomanagement und Compliance.**
Krzysztof Müller (Telekom Austria)
Rudolf Kochesser (Telekom Austria)

11.30 **Sicherheitsarchitektur – Der Bauplan für Sicherheit**
Johannes Mariel (Bundesrechenzentrum GmbH)

12.00 **Rechtsvortrag angefragt**

12.30 **Pause**

13.00 **»Der Weg und das Ziel«: Informationssicherheit nach ISO 27001 effizient umsetzen**
Robert Jamnik (CIS-Zertifizierungsauditor)

13.30 **Web Security**
Andrea Nowak (Austrian Research Centers GmbH – ARC)

14.00 **Weitere Vorträge angefragt**

16.00 **Ende der Veranstaltung**

Das SANS Institute (SysAdmin, Audit, Network, Security) hat in dieser Woche seine Prognose der Top Ten Cyber-Sicherheitsbedrohungen für das angelaufene Jahr 2008 veröffentlicht. Insgesamt zwölf Sicherheitsexperten unter Führung von SANS-Institute-Präsident Stephen Northcutt waren an der Erstellung der Liste beteiligt, die unterstreicht, dass bekannte Angriffsvektoren auch in diesem Jahr von höchster Bedeutung sein dürften.

Platz eins auf der Liste nehmen immer gefinkeltere Website-Angriffe auf Sicherheitslücken im Browser und Browser-Plug-Ins ein. Speziell Plug-Ins wie Flash oder QuickTime sieht die Experten-Runde als lohnende Angriffsziele, da diese beim Browser-Update nicht automatisch gepatcht werden. Dies stimmt mit der Warnung von Secunia-Sicherheitsexperten überein, dass über 95 Prozent aller Nutzer durch nicht gepatchte Software eigentlich behobenen Sicherheitslücken ausgesetzt seien. SANS warnt besonders vor Angriffsmethoden, die eine größere Zahl bekannter Sicherheitslücken betreffen und so ihre Chancen verbessern, Systeme tatsächlich zu treffen.

An zweiter Stelle reiht die SANS-Gruppe verbesserte Botnetze. Auch andere Sicherheitsexperten warnen vor der Wahrscheinlichkeit neuer Botnetz-Massenangriffe. Immerhin ist bekannt, dass Behörden diese spezielle Art der Bedrohung sehr ernst nehmen und etwa das FBI auch groß angelegte Aktionen gegen Cyberkriminelle in internationaler Zusammenarbeit durchgeführt hat und weiter durchführt.

Auf Platz vier der SANS-Prognose finden sich Bedrohungen gegen Mobiltelefone, insbesondere das iPhone und Googles Android. Dieser Einschät-

zung dürften sich nicht alle Experten anschließen, speziell beim Sicherheitsanbieter G Data wurde noch Ende November 2007 davon gesprochen, die Virengefahr für Handys sei »eine große Luftblase«. Auch Voice-over-IP-Angebote könnten laut SANS massiv angegriffen werden. Das an fünfter Stelle gereihte Risiko betrifft speziell Unternehmen und Organisationen: Die Expertengruppe warnt vor Insider-Angriffen.

Weiters folgen in der SANS-Reihung Identitätsdiebstahl durch langfristig aktive Bots sowie zunehmend bösartige Spyware. Erst an achter Stelle folgt die Ausnutzung von Sicherheitslücken in Web-Anwendungen. Zwar ist das SANS Institute der Ansicht, dass entsprechende Angriffsvektoren wie unter anderem Cross-Site-Scripting (XSS) bisher wenig Bedeutung hatten, da Cyberkriminelle auf anderen Wegen leichter zu Erfolgen kamen. Im Jahr 2008 könnten entsprechende Methoden aber einen Aufschwung erleben.

Geschicktere soziale Angriffe reiht das SANS Institute an die neunte Stelle. Neben Phishing mit besserem Kontext – etwa gefälschte Jobangebote, die von bekannten Jobbörsen zu kommen scheinen, wird hier speziell »Event-Phishing« rund um wichtige Ereignisse angeführt. So könnten etwa E-Mails mit Inhalten, die vermeintlich die US-Präsidentenwahl betreffen, großen Erfolg als Methode zur Erstellung von Botnetzen haben. Am Ende der Vorhersagen-Liste finden sich Angriffe über die Vertriebskette, wo Geräte mit Malware ausgeliefert werden. Im Jahr 2007 gab es solch einen Vorfall etwa bei einem USB-Stick aus dem Hause Sony.

Quelle: Pressetext Austria

Einfluss von Gesetzen und Verordungen auf IT-Revision und -Security

- Aufzählung und Kurzerklärung der wichtigsten Gesetze, Verordnungen, die auf IT-Revision/ IT-Security Einfluss haben
- »Ewiges Spezialthema«: Aufbewahrung von Daten, die nicht »direkt« in der Buchhaltung gespeichert sind ⇢ Welche Gesetze, welche Ableitungen, … (Worauf kann man sich beziehen?) und vor allen Dingen: welche Auswirkungen bei Nichteinhaltung.
- Aufbewahrungspflicht und Aufbewahrungsdauer von Logfiles, unter besonderer Berücksichtigung von Identifikationsdaten und Authentifizierungsdaten des Betriebssystems als Zugriffsdaten auf das Netzwerk

Identity Management als Schlüssel zur IT-Governance

Peter Weierich
(Völcker Informatik AG)

Helmut Taumberger
(Fujitsu Siemens)

Welche Person hat(te) wann Zugriff auf welche IT-Ressourcen, Verzeichnisse, Dateien etc.? Nur ein ganzheitliches Identity Management kann diese Fragen sicher beantworten helfen. Im Vortrag beleuchten wir zahlreiche Facetten: Verwaltung der Identitäten und deren IT-Berechtigungen, Account und Compliance Reporting, bis hin zur integrierten Fileshareverwaltung. Abgerundet wird der Vortrag mit einem Erfahrungsbericht aus einem aktuellen Projekt.

Secure Identity Management – soviel Sicherheit muss sein!

Lucas Pachler
(Raiffeisen Informatik GmbH)

Raiffeisen Informatik GmbH hat als Vorreiter in Österreich nun schon die zweite vollständige Lösung zum Thema Secure Identity Management (Identity Management, Single Sign On, PKI mit Smartcard Login) umgesetzt. Die jüngste Lösung ist seit Oktober 2007 bei Raiffeisenkassen im Einsatz und stellt eindrucksvoll unter Beweis, dass Sicherheit und Benutzerkomfort keine sich ausschließenden Themen sind, sondern moderne Arbeitsplatzkonzepte perfekt ergänzen. Der Vortrag geht auf die umgesetzte Lösung und das Leistungsangebot der Raiffeisen Informatik sowie auf die Herausforderungen bei der Einführung dieses Identity Management Konzeptes ein.

IT in Balance – Bedeutung von Risikomanagement und Compliance

Krzysztof Müller
(Telekom Austria)

Das Management von IT ist sehr vielfältig. Es gilt hier mehrere Aspekte gleichzeitig zu berücksichtigen und die vorhandenen Ressourcen optimal einzuset-

zen. Das schnelle und richtige Erkennen der Schwerpunkte und des Bedarfs ist ein Balanceakt. Hilfe kann hier ein pragmatisches Risikomanagement schaffen, dass die Fokussierung aufs Wesentliche ermöglicht. Wichtig ist dabei auch, das Potenzial der Compliance-Tätigkeiten fürs Unternehmen zu erkennen und daraus einen internen Nutzen zu ziehen.

Rudolf Kochesser
(Telekom Austria)

Sicherheitsarchitektur – Der Bauplan für Sicherheit

Die Abbildung des Sicherheitskonzepts in einer Enterprise Architektur erfolgt über eine Sicherheitsarchitektur. Diese stellt die technische Darstellung des Sicherheitsregelwerks für Architekten und Lösungsentwickler zur Verfügung.

- Inhalt und Aufbau einer SiArch
- Positionierung in Sicherheitskonzeption und EArch Zielgruppen und
- Nutzen einer SiArch

»Der Weg und das Ziel«: Informationssicherheit nach ISO 27 001 effizient umsetzen

Die Vorteile von Informationssicherheits-Managementsystemen nach dem Weltstandard ISO 27 001 sind für immer mehr Unternehmen essentiell. Das große Fragezeichen ergibt sich aber bei der zielgerichteten Umsetzung, vor allem in Bezug auf eine angestrebte Zertifizierung. CIS-Auditor Robert Jamnik beleuchtet in seinem Vortrag Erfolgsfaktoren und typische Stolpersteine auf dem Weg zu Hochsicherheit: Wie kann Security-Management effektiv und gleichzeitig kostenschonend aufgesetzt werden? Weniger ist oft mehr – das gilt auch für Kontrollziele im Rahmen der ISO 27 001, wenn sie dafür umso schärfer konturiert und dadurch besser steuerbar werden. Risikoanalysen zielsicher durchführen, Richtlinien »lebbar« formulieren, Handbücher richtig erstellen – Robert Jamnik vermittelt Schlüsselaspekte aus seiner langjährigen Erfahrung.

Robert Jamnik (CIS-Zertifizierungsauditor)

CIS-Lehrgang

ISO 20 000 Consultant

Implementieren, steuern und verbessern von IT-Service-Management-Systemen

Referent:
Markus Schiemer (Quality Austria, CIS)

Der ISO-20 000-Consultant ist ein sich neu etablierendes Berufsbild, bei dem Technologie- und Managementwissen gleichermaßen gefragt sind. Aufbauend auf der IT Infrastructure Library, ITIL, hat das Managementsystem der ISO 20 000 die Verbesserung von Effizienz, Transparenz und Qualität von IT-Leistungen zum Ziel. Als ISO-20 000-Consultant können Sie somit zur Schaltzentrale für Veränderungen und kontinuierliche Verbesserung von IT-Prozessen im Unternehmen werden. Implementierung, Optimierung und die interne Vorbereitung auf Audits gehören zu Ihren Kompetenzen. Die CIS ist die erste, durch den itSMF akkreditierte Trainings- und Zertifizierungsorganisation in Österreich.

Inhalte des dreitägigen CIS-Lehrgangs »ISO 20 000 Consultant«:

- Einführung und Inhalte der ISO 20 000
- Überblick über das Zertifizierungsverfahren
- ISO 20 000 Einführung: Begriffe, Prozesse und Merkmale
- ISO 20 000 Teil 1, im Detail: The Specification for Service Management
- ISO 20 000 Teil 2, im Detail: The Code of Practice
- Einsatz von Service-Management-Tools
- ISO 20 000: Geltungsbereiche
- Implementierung der ISO 20 000
- Praktische Übungen zur Anwendung der ISO 20 000
- Vorbereitung für Assessments und das interne Audit
- Vorbereitung auf die schriftliche Prüfung
- Schriftliche itSMF-Prüfung: 1 Stunde Multiple Choice und 1 Stunde Written Assignment (Praxisanwendungsbeispiele in englischer Sprache)

Die Inhalte dieses dreitägigen Lehrgangs entsprechen den Richtlinien des itSMF UK.

Zielgruppe

Consultants oder Projektmanager, die Organisationen auf die Zertifizierung nach ISO 20 000 vorbereiten.

Voraussetzungen

- ITIL Foundation Certificate in IT Service Management (ITSM)
- gute Kommunikationsfähigkeiten
- 3 Jahre Berufserfahrung in der IT
- 3 Jahre Berufserfahrung in Implementierung / Betrieb von Service-Management-Prozessen oder -Projekten.

Abschluss

Teilnehmer, die dieses Seminar abgeschlossen haben, erhalten ein offizielles »ISO 20 000 Consultant Certificate« des itSMF UK.

Sie sind in der Lage durch ihr tiefes Wissen die Anforderungen der ISO 20 000 in einer Organisation zu implementieren, diese auf die Zertifizierung vorzubereiten und den kontinuierlichen Verbesserungsprozess innerhalb der Organisation effizient voranzutreiben.

Termine:	CB070827	**16.–18. April 2008**
	CB070828	**5.–7. November 2008**
Ort:	Wien, Hotel Stefanie, Hotel Am Parkring	
Gebühr:	Gesamter CIS-Lehrgang »ISO 20 000 Consultant« inklusive Prüfung und Zertifikat: € 2.460,–	
	Alle Preise zuzüglich 20 % MWSt.	

Seminar

Information-Security-Manager

Technologieexperte mit Führungsqualitäten mit Zertifizierungsprüfung nach ISO 27 001 / ISO 27 002

Referenten:
Günther Schreiber (Quality Austria, CIS),
Herfried Geyer (Siemens IT Solutions and 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 ISO 27 001 / ISO 27 002

Aus Risiko wird messbare Sicherheit

Dieses Zwei-Tages-Modul vermittelt Ihnen das Fundament, auf dem moderne ISM-Systeme aufbauen: die Norm ISO 27 001 / ISO 27 002 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:	CB070825	**10.–13. März 2008**
	CB070826	**5.–8. Mai 2008**
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 ISO 27 001 / ISO 27 002

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 1000 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:	CB070824	**9.–11. Juni 2008**
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

Bitte merken Sie sich den Termin für unsere Herbst-Veranstaltung vor:
Security II am 18. 9. 2008

Zielgruppe:
Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand, IT-Entscheider, IT-Verantwortliche, IT-Revision, Compliance-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.

CON•ECT EVENTMANAGEMENT

Anmeldung

☐ Ich melde mich zu »Sicherheitsmanagement, Identitymanagement und Recht« am 21. Februar 2008 an:

- ☐ Kostenfreie Teilnahme als IT-Anwender.
- ☐ Als IT-Anbieter und Berater zu € 390,– exkl. 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
08019