Information Systems Audit and Control Association

News Letter

Nr. 69, Juni 2004

Thema euroCACS2004

Switzerland Chapter
Germany Chapter
Austria Chapter

© 7.6.2004

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni,
8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem *NewsLetter* nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Abo-Preis:
Mitglieder gratis
Abonnemente und Einzelnummern auf Anfrage

Inserate:
1 Seite CHF 400.–
1/2 Seite CHF 240.–
1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich
Auflage: 1100 Exemplare

Nächste Ausgabe (Thema: Professional Judgement in der IT): September 2004, Redaktionsschluss: 20. August 2004

Inhaltsverzeichnis

Editorial 4

euroCACS2004 – Im Zeichen von IT-Governance, Effizienz und Effektivität 6

euroCACS2004 – Was mich aus der Key-Note Speech beeindruckte 7

euroCACS2004 – Using Data Gathering and Analysis Tool 8

euroCACS2004 – Audit als Risikomanager in IT-Projekten? 10

euroCACS2004 – Bewirtschaften von Informations- und Kommunikations-Technologie- Risiken zur Erreichung der Geschäftsziele 12

euroCACS2004 – Rosinen aus dem euroCACS2004-Kuchen 14

Sarbanes Oxley Act – Wächst jetzt der Druck auf das IT-Management? 19

The ISACA Crossword Puzzle 22

Express Line 24

DACH-News 25

Veranstaltungen 28

Germany Chapter 30

Austria Chapter 31

Switzerland Chapter 32

Editorial

Die *euroCACS 2004* in Zürich-Kloten gehört seit einiger Zeit der Vergangenheit an. An der Konferenz wurden viele brisante und interessante Dinge debattiert. Zum Beispiel, ob der Rheinfall wirklich der mächtigste Wasserfall Europas ist, denn an dessen Kopf wurde das Gala-Dinner serviert und zu dessen Fuss ein nächtliches Fackelabenteuer erlebt.

Im Ernst: Etliche Teilnehmer fragten sich, was die Zukunft des „IT-Auditors" sei, warum man sich mit dem Sarbanes-Oxley-Act intensiv beschäftigen müsse, und worum es beim Stichwort *IT-Governance* überhaupt geht, und letztlich, wie es um die Sicherheit bei drahtloser Kommunikation bestellt ist. Die Veranstaltung war in vier sogenannte *Streams* gegliedert:

- IT Assurance Core Competences
- IT Assurance Issues
- Information Security Management
- IT-Governance

Den Teilnehmern war es freigestellt, welche *Sessions* sie im einzelnen besuchen wollten. Der *NewsLetter* widmet die letzte und diese Nummer den Topics der *euroCACS2004*. Teilweise werden Auszüge aus einzelnen *Sessions* beleuchtet. Daneben sollen aber auch Beiträge erscheinen, welche nicht direkt an der Konferenz präsentiert wurden.

Die letzte Ausgabe hatte *IT Governance* zum Schwerpunkt. Die Beherrschung der Informatik war schon immer ein Anliegen der Informatikrevisoren, doch erhielt das Thema erst vor wenigen Jahren mit diesem Schlagwort die ihr zustehende Beachtung. Verschiedene Eclats der letzten Zeit (Enron, Parmalat, Adecco, Sarbanes-Oxley, neue SEC-Bestimmungen, SWX, etc. – die Dunkelziffer schlummernder Bomben dürfte wohl noch in Jahren zu „Explosionen" führen –) zogen die Frage ins Rampenlicht, ob die Wirtschaftsführer wirklich am Steuerrad stehen oder ob sie geführt werden. Dass die Informatik und damit zusammenhängend die Kommunikationsmittel eine prominente Rolle spielen, ist leider noch nicht überall klar. Die Konferenz zeigte Perspektiven auf, welche dieses Manko zwar nicht zu beseitigen wussten, ihm jedoch merklich entgegentraten.

Die vorliegende Nummer behandelt in erster Linie die Topics der übrigen drei *Steams*, wobei die Präsentatoren aus unserem Raum sich nochmals zu ihrem Thema äussern.

Ich wünsche Ihnen bei der Lektüre dieses *NewsLetters* mit dem Schwerpunktthema *euroCACS2004* viel Spass.

Max F. Bretscher

L'euroCACS2004 de Zurich appartient déjà au passé mais les traces des débats passionnés qui s'y sont déroulés subsistent dans nos mémoires. Par exemple savoir si les chutes du Rhin de Schaffhouse constituent bien la plus importante cascade d'Europe. Le dîner de gala qui y a été organisé et une aventureuse promenade au flambeaux ont permis aux participants de découvrir ces chutes dans un cadre très impressionnant.

Revenons aux choses sérieuses. Beaucoup de participants sont venus avec des questions très actuelles : quel est l'avenir de l'audit informatique ? pourquoi sommes-nous concernés par la loi Sarbanes-Oxley ? que couvre l'IT Governance ? quels sont les défis en terme de sécurité que posent les nouvelles technologies de communication sans fil ? Toute la manifestation était organisée en quatre « streams » :

- IT Assurance Core Competences
- IT Assurance Issues
- Information Security Management
- IT Governance

Les participants étaient libre de suivre l'une ou l'autre des très nombreuses sessions des ces quatre streams. Ce numéro de la *Newsletter* est consacrés à *l'euroCACS2004*. Des extraits de certaines sessions mais également des contributions originales sur le thème qui n'ont pas pu être présentées lors de la conférence.

Nous avions déjà traité le thème de l'*IT Governance* dans notre dernière édition. Plusieurs évènements de ces derniers mois (Enron, Parmalat, Adecco, Sarbanes-Oxley, nouvelles

dispositions SEC, SWX, etc. plusieurs bombes à retardement devraient venir allonger cette liste ces prochaines années) ont donné raison aux auditeurs informatiques qui mettent les entreprises en garde depuis des années contre les risques liés aux technologies de l'information. La question centrale n'est plus seulement : y a-t-il un pilote dans l'avion ? mais le pilote maîtrise-t-il son appareil ? Plusieurs sessions de la Conférence ont apporté du matériel qui pourrait aider les pilotes à mieux comprendre les liens entre le pilotage et l'informatique.

Nous nous concentrons donc sur les trois autres thèmes, complétés par les contributions des membres suisses de l'ISACA.

Je vous souhaite une agréable et intéressante lecture de ce numéro spécial *euroCACS2004* !

Max F. Bretscher

Information Systems Audit and Control Association®

An alle ISACA-Mitglieder und Interessenten für Weiterbildung

Der Vorstand von ISACA Switzerland Chapter lädt Sie zu speziellen "After Hour"-Seminaren ein, die jeweils an einem Mitwoch von 16.30 bis 18.00 Uhr mit anschliessendem Apéro und Diskussion stattfinden. Kursort ist Zürich in der Nähe des Hauptbahnhofs. Für ISACA-Mitglieder sind diese Anlässe gratis, Nicht-Mitglieder bezahlen direkt vor Ort Fr. 50.- pro Anlass. Wir bieten Ihnen vorerst folgende Anlässe an:

Datum	Thema	Referent	Ort	Zeit
30.06.04	IT Risk Management	Bruno Wiederkehr	Landesmuseum Zürich	16.30-18.00 Uhr
25.08.04	IT Self Assessment am Europäischen Rechnungshof	Michel Huissod	Landesmuseum Zürich	16.30-18.00 Uhr

Weitere Anlässe finden am **7.07.04, 2.09.04, 20.10.04, 17.11.04** statt. Die Themen und Referenten dieser Daten sind noch nicht bekannt. Bitte schauen Sie auf unserer Webseite **www.isaca.ch** nach.

Für weitere Informationen und Anmeldungen kontaktieren Sie bitte unser Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG, Konradstrasse 1, 8005 Zürich,
kurse@isaca.ch, Tel. 01 440 33 64, Fax 01 440 33 61

www.isaca.ch

euroCACS2004

Im Zeichen von IT-Governance, Effizienz und Effektivität

Zum 15-jährigen Jubiläum des ISACA Switzerland Chapters hat der Vorstand die Gelegenheit wahrgenommen, die europäische Konferenz in Zürich durchzuführen. In der Zeit vom 21. bis 24. März 2004 kamen 280 Teilnehmende aus 40 Ländern ins Hotel Hilton Airport nach Zürich. Trotz der angespannten Wirtschaftslage kamen viele Professionals aus den Bereichen Management, Consulting, Controlling, Informatik, Sicherheit, Recht, Internal Audit, Wirtschaftsprüfung und Ausbildung nach Zürich.

Die 18. euroCACS (Conference on Computer Audit, Control and Security) stand im Zeichen der IT-Governance in Bezug auf Steigerung der Effektivität und Effizienz. Mit einbezogen wurden auch die zunehmende Wirtschafts- und Computerkriminalität sowie die Risiken bei terroristischen Anschlägen.

Die Konferenz wurde durch einen hervorragenden „Keynote Speaker", Herrn Bruno Porro, Chief Risk Officer der Swiss Re, eröffnet. Damit wurde die Ausgangslage geschaffen und der Zusammenhag zwischen dem Geschäfts- und Informatikbereich auf den Punkt gebracht.

Renommierte Referenten vermittelten ihr praxisorientiertes Fachwissen in Vorträgen, Plenum-Gesprächen und Business Cases. Dadurch entstand den Teilnehmenden die Möglichkeit, konkret von den Beispielen in ihrem Berufsalltag profitieren zu können.

Zum guten Gelingen der 40 Sessions und sechs Workshops haben die Sponsoren, Aussteller, Referenten und freiwilligen Helfer beigetragen, denen der gesamte Vorstand des ISACA Switzerland Chapters hiermit nochmals den bestens Dank aussprechen möchte.

Inhalt und Herausforderung

Die Referate wurden in vier Hauptthemen (Streams) basierend auf die strategische Ausrichtung der ISACA gegliedert. Es handelte sich um die folgenden Schwerpunkte:

1. IT Governance: Beherrschung der Informationstechnologie mit Fokussierung auf die COBIT-Beurteilungskriterien und Implementierungsansätze
2. IT Audit & Control Compentences: Methoden, Techniken und Vorgehensweise hinsichtlich IT Audit, Kontrolle und Risikomanagement
3. Information Security Management: Rolle und Aktivitäten im Bereich der System-, Applikations- und Informationssicherheit
4. IT Assurance Issues: Gewissheit und Zusammenarbeit der Audit-, Sicherheits- und Kontrollfunktionen in Bezug auf das Interne Kontrollsystem.

Aus diversen Referaten ging hervor, dass die IT-Governance klar als Teil der Corporate Governance betrachtet wird. Obwohl die inhaltliche Trennung der Kriterien und Aktivitäten nicht immer einfach und sinnvoll ist, gehen nach heutiger Auffassung und Lehre der IT-Governance zwei Hauptrichtungen hervor:

- Mit IT-Ressourcen Werte schaffen, d.h. führen, steuern, messen, Chancen realisieren
- IT-Risiken bewirtschaften, in weiterem Sinne Risiken, Massnahmen und Kontrollen managen.

Als Standard wurde das COBIT-Rahmenwerk von verschiedenen Referenten genannt, welches auch bezüglich Implementierung und Erfahrung weltweit am häufigsten Verwendung findet. Die Management Guidelines von COBIT können sowohl als Überwachungs- als auch als Messinstrument (Balanced Scorecard) der 34 IT-Prozesse eingesetzt werden.

Fazit: What cannot be measured, cannot be managed successfully!

Ausblick

Aus verschiedenen Zusammenfassungen ging hervor, dass IT-Governance und IT-Risikomanagement sowohl von grossen und mittleren, als auch von kleinen Unternehmungen auf ein angemessenes Niveau gebracht werden müssen. Idealerweise lassen sich hier viele Kriterien aus dem erwähnten COBIT-Rahmenwerk und den Management

Guidelines ableiten, wie z.B. kritische Erfolgsfaktoren, Schlüsselziele und Leistungsindikatoren.

Aus den Vorträgen konnten Entwicklungen erkannt werden, welche sich immer neuen Herausforderungen in Bezug auf ein flächendeckendes Informations-, Kommunikations- und Datenrecht stellen müssen. Zur Erfüllung dieser Forderung sind dabei weitere Brücken zu schlagen zwischen

- Informations- und Kommunikations-Technologie (ICT),
- Datensicherheit/Information (Security) und Schutz der Privatsphäre (Privacy),
- Internationalem und nationalem Recht (Regulative, Normen und Verordnungen),
- Steigenden ICT-Risiken und ausgewogenen Gegenmassnahmen,
- Theoretischen Auseinandersetzungen und praktischen Lösungen.

Zu den erwähnten Schwerpunkten stehen den weltweit rund 30 000 ISACA-Mitgliedern eine Vielzahl von Standards, Präsentationen, Downloads von White-Paper, Fachartikeln und -büchern sowie Ausbildung und Zertifizierung zu günstigen Konditionen zur Verfügung. Angaben dazu erhalten Sie unter der Head-office-Homepage www.isaca.org.

Die COBIT-Kontrollziele (Englisch/ Deutsch) und die Management Guidelines (Englisch) können als PDF von der Homepage www.isaca.ch heruntergeladen werden.

Bruno Wiederkehr, ICT Consulting & Training, Erlenbach

euroCACS2004

Was mich aus der Key-Note Speech beeindruckte

Bruno Porro ist der derzeitige Chief Risk Officer der Swiss Re. Er gab in bescheidener Art und Weise zu, nicht ein Experte auf allen Gebieten des Risk-Managements und der IT-Governance zu sein. Er sieht seine Rolle in erster Linie in der Koordination und der Vorbereitung zur Entscheidungsfindung sowie der Überwachung der darauf folgenden Umsetzung. Das vor einigen Jahren vorgenommene Self-Assessment der Swiss Re bezüglich der Sicherheitsfragen (basierend auf BS7799) ergab einen beträchtlichen Nachholbedarf bei sehr vielen Aspekten, wie der gezeigte Spidergraph illustrierte. Daneben sind es aber die gestiegenen Anforderungen an die Computerwelt der letzten Jahre. So sei ihm vor 15 Jahren gesagt worden, die Operationen der Swiss Re könnten problemlos eine Woche ohne IT überleben. Gemäss einer kürzlich durchgeführten Umfrage sei es ein Tag, in gewissen Abteilungen noch weniger. Damit rückt nicht die IT an sich, aber ihr kontinuierliches Funktionieren, auf eine strategische Ebene. Eine Dimension, die weder nebensächlich behandelt, noch bedenkenlos ausser Haus vergeben werden kann.

Max F. Bretscher

euroCACS2004

Using Data Gathering and Analysis Tool

Les objectifs de cette session, qui s'adressait principalement à des débutants, étaient les suivants :

- Comprendre pourquoi l'utilisation d'un outil d'analyse des données peut être un atout.
- Démonstration d'un progiciel d'analyse des données.
- Utilisation de certaines fonctions intégrées.
- Démontrer à l'aide d'exemples pratiques l'utilisation d'un outil d'analyse des données.
- Comprendre les avantages et de la valeur ajoutée liés à l'utilisation d'un progiciel d'analyses de données.

Le progiciel ACL[1] a été retenu pour la démonstration car il est l'outil retenu par les conférenciers dans leur activité professionnelle. D'autres progiciels, fournissant des fonctionnalités similaires, sont également disponibles sur le marché.

Chaque système, informatique en l'occurrence, développe une caractéristique nommée entropie. L'entropie est la tendance qu'a tout système à tendre vers le désordre. L'approche par les anomalies, les tendances ou les cas limites permet de rechercher l'entropie du système à auditer.

Pourquoi utiliser un outil informatique ?
Voici quelques avantages qui peuvent pousser l'auditeur vers l'automatisation de ses investigations:

- facilité d'utilisation : le travail sur les données est facilité grâce à l'existence de quelques commandes permettant d'exécuter la plupart des traitements,
- dépasser le stade du sondage, utilisation de toutes les données à disposition pour effectuer des requêtes,
- le temps gagné permet à l'auditeur de se pencher plus longuement avec son client,
- les fonctions d'historique (fonctionnalités utilisées et résultats obtenus) permettent une traçabilité des étapes de l'audit,
- préservation de l'intégrité des données en ne permettant pas leur modification (intangibilité),
- l'analyse des données se fait de manière interactive et l'auditeur obtient un résultat en temps réel,
- la reprise et la conversion des données : possibilité de traiter un grand nombre de formats de données,
- respecter les normes standard[2] de l'ISACA comme : 060.020 Evidence, 050.010 Audit planning et 030.020 Due professional care.
- effet de prévention. L'utilisation d'outils dans le cadre d'un audit peut prévenir par exemple la fraude.

Le champ d'application de ces outils est très vaste; nous pouvons tout aussi bien faire une comparaison de fichiers provenant de différents systèmes, afin de tester la migration des données, qu'analyser un fichier log ou bien même faire une analyse typique liée aux processus de l'entreprise (clients, fournisseurs, paiements, achats, salaires, etc.).

Il est important de noter que l'utilisation du progiciel devrait être discutée dans la phase de préparation de l'audit. Ceci afin de permettre au client d'extraire les données nécessaires à l'analyse à temps. Typiquement dans cette phase, mais de préférence pendant toute la révision, une grande synergie est nécessaire à l'intérieur de l'équipe multidisciplinaire (réviseur informatique et réviseur financier par exemple).

La méthodologie suivante peut être suivie pour les procédures préalables (Prise en compte de l'environnement informatique et incidence sur la démarche d'audit, CNCC[3], avril 2003):

- S'assurer que les critères choisis seront probants par rapport à l'objectif visé par le test,
- protéger les données initiales et conserver la piste d'audit,
- mettre en forme et classer les données :
  - agrégation
  - tri
  - création d'un fichier à partir d'un autre en reprenant certains enregistrements et certains champs clés,
  - mettre plusieurs fichiers les uns à la suite des autres dans un nouveau fichier
- analyser les résultats :
  - disposer de statistiques sur une valeur (moyenne, somme et nombre de valeurs positives et négatives, dispersion, etc.),

– insérer un champ calculé dans le fichier,
– sélectionner statistiquement des données dans le fichier,
– rapprocher deux fichiers disposant d'une même clé,

- présenter les résultats :
  – éditer les résultats
  – exporter les champs utiles dans un nouveau fichier.

Une partie pratique a été présentée en utilisant un fichier « Paiements »[4]. Les objectifs de l'audit ont été présentés. Pour chaque objectif, le type d'analyse a été expliqué à l'aide d'une démonstration.

Les étapes suivantes ont été démontrées à l'aide de l'outil:

- Contrôle de l'intégralité du fichier à traiter en comparant le total des enregistrements entre le fichier en production et le fichier reçu
- Détection des anomalies et mise en évidence des zones à investiguer
- Classement des informations par ordre chronologique
- Détection des relations employées/fournisseurs suspectes
- Détection des doubles paiements, des trous dans la numérotation des factures
- Vérification des soldes
- Présentation des résultats sous forme de fichier, de tableaux ou de graphes

Les fonctions suivantes, les plus utilisés, ont été expliquées:

- *Stratify* – pour compter le nombre d'enregistrements inclus dans des intervalles spécifiques (strates) de valeurs de champs ou d'expressions numériques, ainsi que pour cumuler un ou plusieurs champs pour chacune des strates
- *Classify* – pour compter le nombre d'enregistrements correspondant à chaque classe unique d'un champ caractère et pour cumuler les totaux des champs numériques indiqués pour chaque valeur.
- *Benford* – cette commande compte le nombre d'occurrences de chaque chiffre à gauche ou d'une combinaison de chiffres, dans un ensemble de données, et effectue la comparaison entre le compte effectif et le compte probable. Le compte probable est obtenu au moyen de la formule Benford. Les outils d'analyse numérique tels que la commande Benford permettent aux auditeurs et aux autres analystes de données de se concentrer sur des anomalies possibles, dans de gros ensembles de données. Ils ne décèlent pas la présence d'une erreur ou d'une fraude, mais ils identifient des éléments méritant une étude ultérieure, sur la base de fondements statistiques.
- *Analyze, sequence, gaps, duplicate* – pour déterminer si les champs-clés dans le fichier courant sont classés dans l'ordre séquentiel et détecter les doublons ou les éléments manquants dans la séquence.
- *Join* – pour combiner des champs (provenant de deux fichiers d'entrée triés) dans un troisième fichier. Joindre généralement est utilisée pour comparer des enregistrements dans un fichier de transaction avec ceux dans un fichier maître.

Donc utiliser un outil d'analyse des données est une méthode d'intégration des principes et des pratiques de la « Business Assurance ». L'expertise dans le domaine de l'analyse des données permet de réduire les risques, de garantir la conformité et la qualité de données, de déceler les indices de fraude, d'améliorer la rentabilité et mieux encore, de bénéficier d'un retour sur investissement rapide.

Massimo Magnini et Eric Rey
Contrôle fédéral des finances, Berne

Annotations

1 ACL= Progiciel pour l'interrogation, l'analyse et le reporting de données, http://www.acl.com

2 Voir le chapitre Standards chez http://www.isaca.org

3 CNCC = Conseil national des commissaires aux comptes, voir http://www.cncc.fr/HTML/main.htm

4 « 101 ACL Applications » by Richard B. Lanza, ISBN 0-9681454-3-4

euroCACS2004

Audit als Risikomanager in IT-Projekten?

Der technologische Wandel und der zunehmende Wettbewerb erfordern, permanent Änderungen an den bestehenden IT- und Kommunikationssystemen vorzunehmen. Die erfolgreiche Bewältigung komplexer IT-Projekte hat in diesem Zusammenhang für die Wettbewerbsfähigkeit von Unternehmen erhebliche strategische Bedeutung erlangt. Ein erfolgreiches Unternehmen muss in der Lage sein, Projekte professionell durchzuführen, um neue Produkte und Dienstleistungen in hoher Qualität zeitgerecht einzuführen. Wie kann die interne Revision ihrer Aufgabe in diesem Umfeld gerecht werden? Welche Anforderungen sind dabei zu beachten?

Die Notwendigkeit eines Risikomanagements in IT-Projekten ergibt sich aus der (auch durch verschiedene Studien belegten) hohen Anzahl von Projekten, die ihr Projektziel nicht erreichen oder erhebliche Zeit- und Budgetüberschreitungen aufweisen. Durch die Einführung eines professionellen Risikomanagements kann solchen Fehlentwicklungen rechtzeitig gegengesteuert werden. Risikomanagement ist daher bereits seit vielen Jahren auch Bestandteil aller wichtigen internationalen Standards für Software-Entwicklung oder Projektmanagement. Heutzutage sollte Risikomanagement in IT-Projekten Bestandteil der unternehmensweiten IT-Governance sein.

Um die Risiken eines IT-Projektes frühzeitig zu erkennen, sollte die Revision im Rahmen ihrer projektbegleitenden Tätigkeit schon bei Projekt-Initiierung darauf achten, dass ein systematisches Projektrisikomanagement eingerichtet ist. Wie aber sieht ein effektives und systematisches Projektrisikomanagement aus?

Das Herzstück eines effizienten Risikomanagements von IT-Projekten ist die systematische Sichtbarmachung der inhärenten Projektrisiken und die Beurteilung der vorhandenen Projektkontrollen. Projektrisiken sind mögliche Bedrohungen für den Erfolg eines Projektes. Inhärente Risiken sind Bedrohungen, die in einem Prozess grundsätzlich existieren, d.h. bevor Kontrollen eingerichtet worden sind. Diese inhärenten Risiken hängen u.a. von der Art des Projektes, des Unternehmensbereiches und der eingesetzten Technologie ab. Die systematische Identifikation der inhärenten Projektrisiken sollte auf einem möglichst umfassenden Risikokatalog basieren, der die Erfahrungen aus vielen Projekten zusammenfasst. Für eine solche Risiko-Checkliste bietet sich eine Kategorisierung in die kritischen sechs Projektbereiche Projektmanagement, Geschäftliche Ausrichtung, Geschäftsprozesse, Anwender, Technologie und Daten an.

Damit eine solche Risiko-Checkliste einheitlich und personenunabhängig eingesetzt werden kann, sollten mehrere Leitfragen für jeden Projektbereich vorgegeben und jede Leitfrage durch Unteraspekte und Beispiele weiter erläutert werden. Eine Leitfrage im Projektbereich Technologie für das inhärente Projektrisiko „Neue Technologie“ lautet beispielsweise: „Hängt der Projekterfolg von Technologien ab, die neuartig sind und mit denen im Unternehmen wenig Erfahrung vorhanden ist?“ Zusätzlich sollte für jede Leitfrage am Ende eine Bewertungsskala für das inhärente Risiko zur Verfügung gestellt werden. Ziel der Analyse ist, für jeden Projektbereich ein inhärentes Bereichsrisiko zu ermitteln, das in der folgenden Phase genauer bewertet wird.

Zur Bewertung der Projektrisiken müssen die Kontrollen in den definierten kritischen Projektbereichen aufgenommen und deren Effektivität beurteilt werden. Die Erfassung und Beurteilung der Projektkontrollen muss natürlich ebenso systematisch erfolgen wie die Identifikation der Projektrisiken. Für jeden Projektbereich sollte dazu anhand von Kontrollfragen und Best-Practice-Beispielen die Effektivität der Projektsteuerungs- und kontrollverfahren bewertet werden. Im Projektbereich Technologie ist ein Vorgehensmodell beispielsweise eine Projektkontrolle, die durch die Kontrollfrage „Erfolgt die Software-Entwicklung nach einem einheitlichen Vorgehensmodell?“ angesprochen wird. Weitergehende Erläuterungen und Hinweise auf idealtypische Nachweise (zum Beispiel

Dokumentation des Vorgehensmodells) für die einzelnen Kontrollfragen sollten eine genauere Beurteilung der Wirksamkeit der Projektkontrollen erleichtern.

Durch die Abwägung von bewerteten inhärenten Risiken und existierenden Kontrollen kann das vorhandene Projektrisiko – je nach Bedarf – sowohl für jeden definierten kritischen Projektbereich als auch für jede einzelne Projektbedrohung ermittelt werden. Eine solche skalierbare Risikoeinschätzung erlaubt in der nachfolgenden Phase eine fokussierte Definition und Umsetzung von Maßnahmen.

Auf Basis der ermittelten Projektrisiken können nun gezielt Maßnahmen zur weiteren Risikominimierung festgelegt werden. Hilfreich bei der Priorisierung ist die Bildung eines Risikofaktors, der z.B. ein Produkt aus einem Maßstab (zum Beispiel 1=gering bis 5=sehr hoch) für die Eintrittswahrscheinlichkeit und für die Auswirkung/Schadenshöhe darstellt. Dieser Risikofaktor sollte vor dem Hintergrund der durchgeführten Risikoanalyse und in Diskussion mit den Projektverantwortlichen festgelegt werden, um aus wirtschaftlicher Sicht angemessene Maßnahmen einleiten zu können.

Bei der Festlegung der Maßnahmen kann man sich an der Systematik einer Risikoreduktions-Treppe orientieren, die aus den folgenden abgestuften Maßnahmen-Typen besteht:

- Risikovermeidung (zum Beispiel durch Änderung des Projektumfanges)
- Risikoverminderung (zum Beispiel durch Behebung der ermittelten Kontrollschwächen)
- Risikobegrenzung (zum Beispiel durch Entwicklung von Alternativen im Falle eines Scheitern des Projektes)
- Risikoverlagerung (zum Beispiel durch Vereinbarung von Schadensersatz)
- Risikoakzeptanz

Die festgelegten Maßnahmen müssen in den Projektplan integriert werden und sollten zusätzlich vom Risikomanager überwacht werden. Für die einzelnen Risiken sollte darüber hinaus ein Risikoeigentümer (Risk Owner) festgelegt werden, der auch für die Umsetzung der jeweiligen Maßnahmen und damit für die Bewältigung des Risikos verantwortlich ist.

Jedem IT-Revisor ist klar, dass eine einmalige Risikoaufnahme im IT-Projekt kein ausreichendes Risikomanagement darstellt. Vielmehr sollte die Beurteilung der Risiken und Kontrollen über die gesamte Projektlaufzeit hinweg regelmäßig aktualisiert und ggf. weitere Maßnahmen definiert und umgesetzt werden. Ein hilfreiches Instrumentarium in diesem Zusammenhang ist die Definition und Überwachung des Risiko- und Kontrollniveaus mit Hilfe von Risiko- und Kontrollindikatoren, die ein objektives Maß für Veränderungen der Risiko- und Kontrollsituation darstellen. Im Projektbereich Technologie ist beispielsweise die „Anzahl der Schnittstellen“ ein möglicher Risikoindikator für die Komplexität eines IT-Projektes.

Die Erfahrung zeigt, dass das Risikomanagement nicht in der Verantwortung des Projektleiters liegen sollte. Vielmehr sollte im Sinne eines Vier-Augen-Prinzips und zur Vermeidung einer gewissen „Betriebsblindheit“ eine unabhängige Stelle regelmäßig den Status der Projektrisiken und -kontrollen überwachen. Die Revision wird sicherlich nur bei kleineren Unternehmen oder übergangsweise eine geeignete unabhängige Stelle sein. Die Prüfung der Funktion Projektrisikomanagement sollte dagegen regelmäßig im Prüfplan auftauchen.

Markus Gaulke,
KPMG Frankfurt am Main

euroCACS2004

Bewirtschaften von Informations- und Kommunikations-Technologie-Risiken zur Erreichung der Geschäftsziele

Zusammenfassung des Referates an der EuroCACS 2004

Ausgangslage

Der Freudentaumel nach Corporate Governance und IT-Governance (Information and Communication Technology) ist vorübergehend bei vielen Schweizer Unternehmen einer Ernüchterung und einem heftigen Kostensenkungsprogramm gewichen. Doch die Awareness hinsichtlich Risiken und Massnahmen wird heute von jungen Mitarbeitenden als etwas Selbstverständliches empfunden. Weit schwieriger ist es jedoch, ein tragfähiges und wirtschaftlich vertretbares Fundament für ein unternehmensweites Risiko-Management-System zu giessen.

Die aus nächster Nähe bekannten Skandale, Pleiten und Computer-Fehler fordern die oberste Unternehmensleitung auf, abgestimmte Risiko- und Kontroll-Frameworks weiter anzupassen bzw. auszubauen. Gleichzeitig sind die Probleme zu lösen, welche durch die Restrukturierungsprogramme in den Prozessen entstanden sind. Noch zu oft wird Risiko-Management als reines „Verhinderungs-Management“ verstanden. Dabei gilt es, bei der Analyse von Risiken gleichzeitig Chancen zu erkennen und wertschöpfende Massnahmen bzw. Gewinne zu realisieren.

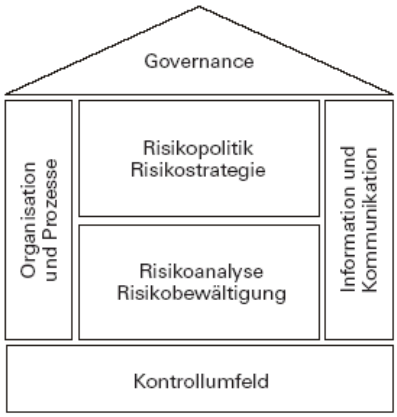
Das Referat setzte sich mit einer breiten Palette von risikobezogenen und risikorelevanten Sachverhalten sowie Fragen auseinander:

- Wie kann ein unternehmensweites Risiko-Management-System gestaltet werden?
- Wer ist für die Initialisierung, Aufgaben (Vision, Strategie, Analyse etc.) und Prozesse verantwortlich?
- Welche Risiko-Methoden, -Techniken, -Werkzeuge und -Verfahren sind einzusetzen?
- Welche Faktoren und Indikatoren sind notwendig, um die Aktivitäten hinsichtlich Risiken zu messen und Massnahmen zu überwachen?
- Welche Anforderungen werden an eine durchgehende Risiko-Management-Kommunikation und an ein periodisches Reporting gestellt?
- Wie kann ein Risiko-Management-System wirtschaftlich implementiert werden?

Aus dem Inhalt

Das Referat bestand aus vier Hauptteilen, welche auf aufgrund der nachstehenden Abbildung zusammengefasst sind:

1. Einflussfaktoren, Governance, Risiko-Vision, -Politik, -Strategie und -Modell
2. Organisation, Risiko-Prozess, -Information und -Kommunikation



3. IT-Risiko-Kategorien, -Analyse und -Bewältigung
4. Kontrollumfeld, Messung und Überwachung der Risiken bzw. Massnahmen.

Der vollständige Inhalt der einzelnen Bauteile kann dem Lehrmittel Modul 246 der Informatik Berufsbildung Schweiz entnommen und unter www.compendio.ch bestellt werden.

Einflussfaktoren

Die Banken und ihre Aufsichtsbehörden haben schon vor einiger Zeit erkannt, dass wirkungsvolle Kontrollmechanismen im Geschäfts- und IT-Bereich von existentieller Bedeutung sind. Regulative wie Turnbull Report, Basel II und Sarbanes-Oxley Act verpflichten den CEO, CFO und CIO, sich über die Wirksamkeit der internen Kontrollen zu vergewissern und diese zu bestätigen.

Dies hat wiederum die Einschätzung und Dokumentation der Risiken in allen relevanten Arbeitsabläufen sowie ein konzernweites Reporting zur Folge.

Ziel und Organisation

Das Governance-Prinzip soll sicherstellen, dass die IT-Risiken im Sinne der Geschäftsziele bewirtschaftet werden. Ein zweckmässiges Risiko-Management-System gehört deshalb zu den grundlegenden Voraussetzungen für eine wirksame und wirtschaftliche Unternehmensführung. Wichtig ist in erster Linie, welche Köpfe, Ideen und Leitplanken hinter der Gestaltung eines Risiko- und Kontroll-Frameworks stecken. In vielen Schweizer Unternehmen schlummert ein enormes Synergiepotenzial, das für die Initialisierung und den Aufbau genutzt werden könnte.

Die Potentiale leiten sich aus bisherigen und neuen Strukturen (z.B. Audit-Committee, Corporate Audit, Controller, Compliance, Projekt-, Risiko- und Qualitäts-Management) ab, deren Tätigkeiten bis heute wenig koordiniert abliefen. Durch klare, aufeinander abgestimmte, Aufträge und intensivere Zusammenarbeit könnten erhebliche Erfolge erzielt werden.

Anwendbarkeit und Nutzen

Mit der Fokussierung auf das Kerngeschäft müssen Risiken und Chancen sowie die engere Zusammenarbeit der Gremien neu hinterfragt werden. Der Fokus liegt einerseits darauf, die Kompetenzen zum Nutzen der Kunden zu verbinden und anderseits mit einem angepassten Risiko Management aufzuzeigen, wo Werte vernichtet oder geschaffen werden können. Auf den Punkt gebracht könnte man sagen: „Manage Risk – Drive Performance“.

Dabei geht es nicht darum, dass Einzelrisiken unabhängig voneinander evaluiert und bewirtschaftet, sondern aus der Perspektive der Unternehmensleitung auf ein adäquates Risiko- und Kontroll-Framework abgestimmt werden.

Mit neuen Ansätzen und klarer Risikostrategie, -Bewältigung, -Messung (Balanced Scorecard) und -Überwachung können die Aktivitäten der erwähnten Organisationseinheiten besser koordiniert und „gemanaged“ werden.

Zukunft und Lessons learned

Sicher ist, dass Vorkommnisse wie bei Enron, Worldcom, Erb, Parmalat und Adecco nie durch Gesetze und regulatorische Auflagen vollständig ausgeschlossen werden können.
In Zukunft werden jedoch die Corporate- und IT-Governance-Kultur einer Unternehmung, die persönliche Eigenverantwortung und Berufsethik der einzelnen Mitarbeitenden wichtige Erfolgsfaktoren sein.

Es ist davon auszugehen, dass die Investoren vermehrt jene Firmen honorieren, welche bereits heute die Risiken im Griff haben sowie die vorerwähnte Kultur leben und dadurch das notwendige Vertrauen der Stakeholder geniessen.

Fazit: Vertrauen ist gut – angemessene Risikoeinschätzung und Kontrollen sind besser!

Rückfragen werden gerne beantwortet via E-Mail:
bru.wiederkehr@bluewin.ch .

Bruno Wiederkehr
ICT Consulting & Training
Erlenbach

euroCACS2004

Rosinen aus dem euroCACS2004-Kuchen

gepickt von Max F. Bretscher

Role of the Information Security Manager (Itamar Mor)

Der Präsentator sieht den Security Manager diversen externen und internen Einflüssen ausgesetzt. Die hauptsächlichen externen sind die gesetzlichen bzw. branchenspezifischen Regulatoren, das Gesetz an sich, die Umwelt, externe Ereignisse, professionelle Standards, Benützer und Geschäftspartner. Von den internen sind besonders zu erwähnen die Benutzer, der Sicherheitsbeauftragte (Security Officer, falls er dies nicht selber ist), der CIO, die Führungsinstitutionen, interne Standards und Ereignisse. Die Diskussion ergibt, dass vom Information Security Manager je nach Standpunkt unterschiedliche Rollen erwartet werden: Detektiv, Polizist, Geheimagent, Bodyguard, Soldat, Politiker, Lehrer, Prophet, Buchhalter, Rechtsanwalt, Vermittler, Ingenieur, Werbemensch, Techniker, und vieles mehr. Der Autor kommt zum Schluss, dass der Information Security Manager am besten Magier oder Zauberer sei. In andern Worten: Die Rolle ist noch nicht eindeutig festgelegt und jeder muss in seiner Umgebung seine Rolle zuerst definieren, bevor er sie wahrnimmt.

Auditing ASP Outsourcing (Abdul Rafeq)

Der Präsentator hat eine grosse Erfahrung auf diesem Gebiet, und dies offenbar auf beiden Seiten. Für ihn sind die folgenden Fragen von ausschlaggebender Bedeutung, ob Verarbeitungen ausser Haus vergeben werden sollen oder nicht, wobei er unterstellt, dass die Fragen mit ja beantwortet werden:

- Ist es eine Kernkompetenz? Kein Outsourcing.
- Wird geplant, die Computer-Infrastruktur in den nächsten zwei Jahren neu zu bauen? Eher Outsourcing.
- Besitzt die Infrastruktur genügend Kapazität (inkl. Bandbreite), um die strategischen Ziele zu erreichen? Kein Outsourcing.
- Plant die Firma eine ERP-Lösung zu installieren? Outsourcing.
- Will die Firma an der Spitze der Technologie mittun? Kein Outsourcing.
- Kann die Firma über mindestens drei Jahre für IT-Personal attraktiv bleiben? Outsourcing.

Der Autor geht sodann auf COBIT ein und weist auf DS 5.4 hin. Besonderes Augenmerk wirft er sodann auf die Problematik der Vertraulichkeit und die Tatsache, dass der Unternehmer letztlich die Verantwortung nie ganz abgeben kann.

Anmerkung der Redaktion: Die IG Outsourcing des Switzerland Chapters hat eine umfangreiche Checklist erarbeitet, die auf der Homepage des Switzerland Chapters www.isaca.ch verfügbar ist.

Making a Business Case for Information Security (Derek Oliver)

Es ist wohl unbestreitbar: Sicherheit kostet Geld. Deshalb schrecken viele Firmen davor zurück, in die Sicherheit (viel) Geld zu investieren. Ergo muss Sicherheit „verkauft“ werden.

Die Entscheidungsträger müssen erkennen, dass viele Drohungen im Umfeld der Informatik bestehen: Betrug und Veruntreuung, Erpressung, Verletzung von Gesetzen, Verletzung von anderen Vorschriften, Imageverlust, Verlust von Kunden, Verlust von Marktanteilen. Und all dies kostet eben (auch) Geld!

Die heutige Welt ist geschrumpft, das internationale Geschäft boomt und die gegenseitige Abhängigkeit nimmt laufend zu. Wie kann man den Geschäftspartnern trauen? Gegenfrage: Können die Geschäftspartner uns trauen?!

Es ist deshalb von eminenter Bedeutung, dass

- die Notwendigkeit der Informationssicherheit eingesehen wird,
- die vorgeschlagenen Lösung auf einem hohen Niveau steht,
- die Vorteile, die Kosten, der Zeitrahmen, die Ressourcen und Risiken festgelegt werden.

Nie darf die Gegenüberstellung von Kosten und Nutzen ausser acht gelassen werden.

Es ist Aufgabe des IT-Revisors, das Management auf die Sachlagen aufmerksam zu machen, nicht aber die Massnahmen zu treffen.

Legacy Interfaces: Where the Past Meets the Future (Jeff Roth)

The author looks back at the Y2K nightmare. Many firms have hastily updated their old legacy systems without properly considering the issues concerning the interfaces with current and past applications. Some had to revert to stand-alone solutions, causing additional interface problems. He draws the attention to the fact that it has been proven that the time necessary to cope properly with interfaces of this nature increases by the square of the number of the interfaces! This observation should be taken into account when embarking on solving interfaces automatically.

A few key issues are addressed: It is a common fact that migrations tend to uncover "skeletons" that have been dormant in the old systems, such as nonnumeric data in assumed numeric fields, fields containing coded information known to the user only, and fields that have to be truncated because of the conversion to ERP systems. The interest of the migrating party to have the acceptance of the user is paramount. Special interest should not only be paid to the migration itself, but also to the "closing procedures" following the migration (month end, quarter, year end) as many snags are revealed only at these times.

Designing Appropriate Information Security Architecture (Pavol Adamec)

Ausgehend von der Theorie über Information Security landet der Präsentator sehr schnell bei den notwendigen Kontrollen und deren Architektur. Die Aspekte der Verfügbarkeit, der Vertraulichkeit und der Integrität müssen durch präventive, entdeckende und korrigierende Kontrollen sichergestellt werden. Sie können auf organisatorischer, logischer und physischer Ebene implementiert werden, sind aber aufeinander abzustimmen. Nur das gesamte Kontrollpaket ist wirksam, einzelne isolierte Kontrollen sind zu vermeiden, da sie sogar oft kontraproduktiv wirken, wie der Autor an einem Beispiel demonstriert.

How to Assess and Manage Information and Technology Risk (John Mitchell)

Es ist dem Präsentator klar, dass es sehr viele unterschiedliche Risiken in der Informatik hat. Er streicht heraus, dass die Wurzelgründe (*root causes*) und nicht die Symptome, angepackt werden müssen. Als Beispiele technischer Natur nennt er Absturz des Servers, ungenügender Speicherplatz, Netzwerkprobleme, ungenügende Bandbreite, USP-Ausfall, Stromunterbruch, Programmfehler.

Am Beispiel der Notstromgruppe (USP) erläutert er, dass laufend messbare Indikatoren zu definieren sind, welche die Situation signalisieren (grün bedeutet, die USP-Anlage wird mit Strom gespiesen, gelb bedeutet, die USP-Anlage ist eingesprungen, weil die Normalversorgung ausgefallen ist, rot bedeutet, die USP kann nur noch eine Stunde den Ausfall überbrücken, usw.

Schliesslich weist auch er, wie viele andere Autoren, auf die Brauchbarkeit des Standardwerkes COBIT hin, das für ein erfolgreiches Risk Management ein wertvolles Werkzeug ist.

Nontraditional Assurance (Kaya Kazmirci)

Als „traditional" bezeichnet der Autor das klassische Testat einer finanziellen Jahresrechnung. Als „nontraditional" versteht er Bestätigungen, welche sich mit andern Sachverhalten auseinandersetzen, z.B. die Bestätigung der Auflage einer Zeitung, Richtigkeit von Konsumentenindices, Verkehrsbeobachtungen bei Internetportalen, etc.

Da die Bestätigungen aus Effizienz- und Kostengründen sich nicht auf eine totale Beobachtungsmenge und -zeit beziehen können, müssen die einschlägigen „Zertifikate" sorgfältig formuliert werden und auf die beschränkte Gültigkeit sowie die angewandten Methoden hinweisen.

Der Präsentator hat selber ausgedehnte Erfahrung auf dem Gebiet in der Türkei und diskutiert den Wert solcher Bestätigungen.

Anmerkung des Redaktors: Die Fachmitteilung Nr. 9 (Zertifizierung von Software) der Treuhandkammer fällt wohl in die gleiche Kategorie.

Auditing Wireless Networks (John Tannahill)

Der Autor stellt fest, dass das weite Publikum bezüglich drahtloser Netzwerke sehr unbekümmert, wenn nicht sogar fahrlässig, geworden ist. So ist das Schnüffeln via „War Driving“ oder „War Walking“ beinahe zum Volkssport geworden: Netzwerkpunkte werden ausfindig gemacht, um einerseits die Gespräche und den Datenverkehr abzuhören, andererseits, diese Punkte auch für eigene (Gratis-)Benutzung zu verwenden. Es ist deshalb notwendig, dass die Übergangspunkte durch mehrfache Firewalls geschützt werden, andererseits die Übermittlung an sich auf sicherer Chiffrierung der Meldungen basiert. Der Referent stellt fest, dass wohl wirksame Standards existieren (z.B. IEEE 802.11a-g), doch leider nicht immer sinnvoll angewendet werden. Er streicht heraus:

- Entwickle eine Politik für drahtlose Netzwerke, bevor Du eines installierst
- Definiere Standards für Zugriffs- und Übergangspunkte
- Definiere den Sicherheitsperimeter und die Netzwerksegmentierung
- Definiere Chiffrierungs- und Authentifizierungsmechanismen
- Stelle Tests bereit, um die Verletzlichkeit zu überprüfen
- Verwende Entdeckungssysteme für Eindringungsversuche (IDS)

Computer Forensics in Motion (Fran Butler)

Obschon es eigentlich nicht die Aufgabe des Revisors ist, kriminelle Tätigkeiten aufzudecken, so kann er doch in solche Situationen geraten. Er ist dann verpflichtet, den Sachen auf den Grund zu gehen. Das kann z.B. dann passieren, wenn der Revisor im Laufe seiner Prüfungen grosse Datenmengen untersucht, und dabei auf „Unstimmigkeiten“ stösst. Daneben ist es möglich, dass ihm ein einschlägiger Auftrag explizit erteilt wird.

Wichtig ist dem Autor, dass beim Vorgehen in solchen Fällen folgende Prinzipien eingehalten werden:

1. Es dürfen keine Veränderungen an den Originaldaten vorgenommen, sondern es muss mit Kopien gearbeitet werden.
2. Nur in absoluten Ausnahmesituationen darf auf der Original-Hardware gearbeitet werden, wobei der Bearbeiter sich über eine hohe Kompetenz ausweisen muss.
3. In allen Fällen muss ein lückenloser Revisionspfad bezüglich der vorgenommenen Tätigkeiten vorhanden sein.
4. Die Nachweispflicht darüber, dass die Daten korrekt behandelt wurden, ist dem Bearbeiter auferlegt.

IT Audit Manager: Tips and Ideas (Panel Discussion)

Schade, dass in solchen interessanten Diskussionsrunden keine Protokollführung stattfand: Dies wäre ein Vorschlag für künftige Konferenzen. Die Ideen und Meinungen, welche spontan präsentiert werden, stehen unmittelbar nur denjenigen Teilnehmern zur Verfügung, welche sich für diese *Session* eingeschrieben hatten. Nun ist es aber nicht möglich, sich für alle Diskussionsrunden einzuschreiben, sei es nur, weil diese teilweise gleichzeitig stattfanden. Immerhin aus dieser Rosine einige Kernaussagen:

- Immer öfter wird die Meinung vertreten, dass der IT-Revisor überflüssig sei, denn er werde durch Systeme ersetzt. Ist damit der IT-Revisor überflüssig? Hat er gar keine Zukunft? Die Antwort liegt wohl darin, dass der „technische“ IT-Revisor wohl bald überholt wird, und vermehrt der IT-Revisions-*Manager* gefragt ist!
- Insbesondere in der internen Revision ist es von ausschlaggebender Bedeutung, dass der Geprüfte mit den Erkenntnissen einverstanden ist: Ja, er sollte selbst die zu treffenden Massnahmen vorschlagen und sich somit mit dem Revisionsbericht identifizieren.
- Misstrauen muss auf jeden Fall abgebaut, wenn nicht ganz eliminiert, werden: Der Revisor muss versuchen, mit den Geprüften eine Vertrauensbasis aufzubauen. Am besten gelingt dies, wenn er sich dauernd bemüht, dem Geprüften (und der Firma) einen Nutzen (*added value*) zu verschaffen.
- Es soll vorkommen, dass der Revisor an ein Problem gerät, zu welchem er selber keinen vernünftigen Lösungsvorschlag vorbringen kann. Dann soll er wenigstens empfehlen, dass der Geprüfte die Sache selbst untersucht und nach Lösungen sucht (*investigate possiblities*).

■ Wenn Expertise gefragt ist, soll auch Expertise eingesetzt werden (*outsourcing*), es ist vermessen, auf jedem Gebiet ein Experte sein zu wollen: Dies ist alles andere als professionell – Und gerade dies wird aber vom IT-Revisor gefordert!

10 Top-Sicherheits-probleme im Unix Bereich

Diese Rosine ist gepickt von Jack Hirschi, CISA, Swiss Federal Audit Office, Bern

Pavol Adamec aus Bratislava identifizierte 10 Top-Sicherheitsprobleme im Unix-Bereich, die er in zwei Kapitel gliederte:

■ Top Vulnerabilities to Unix Systems

■ Top Security Administration Mistakes

Als Grundlage dienten ihm auch Aussagen aus der SANS 2003[1]. Adamec behandelte folgende Schwachstellen bei Unix-Systemen:

BIND/DNS

BIND ist die am meisten verwendete DNS-Implementierung bei Unix-Plattformen. Viele OS-Auslieferungen haben BIND (namentlich) als Defaultwert hinterlegt. Eine grosse Anzahl von Systemadministratoren verwenden nicht die neusten Patches und/oder haben die Unix-Plattform falsch konfiguriert.

Identifikationsmöglichkeiten:

■ Wurde z.B. ein „BIND package“ installiert?

■ Läuft ein „BIND“-Prozess?

■ Überprüfung der aktuell installierten Version (Version 4 zum Beispiel ist veraltet und enthält viele Bugs).

Mögliche Auswirkungen:

■ Denial of service

■ Root compromise

Mögliche Gegenmassnahmen:

■ Disable named

■ Verwendung einer abweichenden DNS-Implementation

■ Upgrade auf die aktuellste Version

■ Hardening (chroot, non-root, etc.)

Remote procedure Calls (RPC)

Viele OS-Auslieferungen installieren RPC-Services mit Defaultwerten (portmapper, NFS, NIS, etc.) und RPC-Services werden normalerweise mit „root privileges“ ausgeführt. RPC stellt nicht nur im MS-Bereich ein Problem dar. Jedes System hat im RPC-Bereich Risiken, die es zu beachten gilt.

Identifikationsmöglichkeiten:

■ Prüfen, ob der „portmapper“-Prozess läuft. Wenn das so ist, wäre dies eine schlechte Nachricht.

■ Mit dem Befehl „rpcinfo-p“ können offene RPC ports and services angezeigt werden.

Mögliche Auswirkungen:

■ Depends of services vulnerabilities

■ Denial of service

■ Root compromise

Mögliche Gegenmassnahmen:

■ Disable RPC services and portmapper (kritischer Parameter)

■ Patch/upgrade services

■ Harden/block/disable RPC services (speziell bei NFS!). Gemäss Aussage von Adamec gibt es keinen Grund, diesen Parameter anders zu setzen.

Apache Web-Server

Es handelt sich hier um einen der populärsten Web-Server. Sowohl der Kern des Apache wie auch die individuellen Module (CGI, PHP, etc.) können ausgenützt werden. Viele OS-Auslieferungen haben defaultmässig Apache installiert. Apache wird durch viele Lieferanten bereits als eingebauter Web-Server mitgeliefert.

Identifikationsmöglichkeiten:

■ Läuft der httpd-Prozess?

■ Sind die „Apache packages“ installiert?

Mögliche Auswirkungen:

■ Denial of service

■ Freigabe von Dateien und anderen Informationen

■ Root compromise

Die Probleme beim Apache Web-Server sind denjenigen des IIS-Servers sehr ähnlich.

Mögliche Gegenmassnahmen:

■ Patch/upgrade Apache core and modules

■ Harden Apache (chroot, PHP/CGI/SSI modules, etc.).

Generelle Unix Authentisierung

Immerwährende Accounts ohne Passwörter oder nur mit schwachen Passwörtern. Viele Systeme beinhalten Accounts mit Default-Pass-

wörtern, die nach der Installation nicht geändert werden.

Identifikationsmöglichkeiten:

- Shadow-Dateien werden nicht verwendet.
- Es existieren Accounts ohne Passwörter.
- Passwort-Crackers werden verwendet.
- Passwortablaufdatum und Grundsätze sind nicht gesetzt.
- Überprüfung anhand der Liste mit bekannten Default-Passwörtern (z.B. http://www.phenoelit.de/dpl/dpl.html).

Mögliche Auswirkungen:

- Blossstellung des Accounts
- Eskalation der Rechte

Mögliche Gegenmassnahmen:

- Definition einer Richtlinie für die Verwendung von Passwörtern
- Verwendung von OS-Features zur Umsetzung der Richtline
- Überwachung auf Vorschriftsmässigkeit

Pavol Adamec ging im Unix Systembereich noch auf folgende Risikobereich ein: Clear Text Services. Viele Services senden Passwort und Inhalt in einem lesbaren Textformat über das Netzwerk wie FTP, telnet, POP3, r-commands, http, SMTP, TFTP, LDAP, SNMP, etc. Bei vielen OS-Auslieferungen sind diese Services default-mässig installiert.

Sendmail, SNMP, Secure Shell (SSH), Falschkonfiguration von NIS/NFS und Open Secure Socket Layer (SSL) gehören ebenfalls zu den 10 Top-Sicherheitsproblemen im Unix Systembereich.

Jeder Risikobereich muss individuell analysiert werden. Oft können mit einer entsprechenden Konfiguration des Systems diese Risiken vermindert oder sogar ganz eliminiert werden.

Bei der Sicherheitsadministration listete Pavol Adamec im Unix-Bereich folgende Schwachstellen auf:

Top Security Administration Mistakes

- „No hardening“, das System wird mit unnötigen Funktionalitäten oder mit einer nicht optimalen Sicherheit betrieben, etc.
- Verwendung von Default-Passwörtern.
- Benötigte aktuelle Patches wurden nicht installiert.
- Unverschlüsselte Protokolle werden für das Management verwendet.
- Via Telefon werden Passwörter ohne saubere Verifikation vergeben.
- Es bestehen keine funktionalen oder gar keine Backups.
- Es laufen unnötige Services auf dem System.
- Es werden falsche Firewall-Regeln angewendet.
- Es ist keine oder keine aktuelle Anti-Virus-Software installiert.
- Und „last but not least“, stellen ungenügend ausgebildete Benutzer das grösste Fehlerpotenzial dar.

Der junge Referent hat mit seiner offenen Art, den beispielhaften Erklärungen und dem gut platzierten Humor das Publikum für sich gewinnen können. Die Sensibilisierung für die 10 Top-Sicherheitsprobleme im Unix-Bereich ist ihm auch zu später Stunde gelungen.

Endnoten

1 SANS: The SANS Institute, Bethesda, Maryland USA; http://www.sans.org/top20

COBIT international

Diverse possibilità di utilizzo di COBIT: esempio italiano

Sarbanes Oxley Act

Wächst jetzt der Druck auf das IT-Management?

Das neue US-Gesetz zur Wiederherstellung des öffentlichen Vertrauens in Kapitalmarktinformationen hat nicht nur Auswirkungen auf die Arbeit der Wirtschaftsprüfer, sondern verlangt auch Massnahmen zur Verbesserung der internen Kontrollsysteme. Der Druck auf die IT wird wachsen. Doch es sind gute Ansätze für ein effizientes und SOA-konformes IT-Management vorhanden – sie müssen nur umgesetzt werden!

Kaum hat die IT-Zunft mit Freude papierfeindliche agile Ansätze der Software-Entwicklung zur Kenntnis genommen, wie zum Beispiel eXtreme-Programming oder SCRUM, schlägt die Bürokratie in aller Härte zurück. Die Hiobsbotschaft kommt aus den USA und heisst Sarbanes-Oxley-Act, kurz SOA. Nach dem Enron-Skandal sind die Gesetzeshüter, unterstützt von reaktionsschnellen Consultants, blitzartig aufgesprungen, um die Gesetze zu verschärfen – gerade noch rechtzeitig, um die sich leerenden Beraterkassen wieder etwas zum Erklingen zu bringen. Das 2002 in Kraft getretene US-Gesetz soll weiteren Bilanzfälschungen einen Riegel vorschieben. Ziel ist es, mittels strenger Bestimmungen zur Corporate Governance das Vertrauen der Öffentlichkeit wieder zu gewinnen. Von den neuen Anforderungen sind nicht zuletzt auch die IT-Abteilungen von in den USA kotierten Unternehmen betroffen.

Prozesse definieren genügt nicht!

Welche Bedeutung hat SOA aber für die Schweiz, oder konkreter: Welche Konsequenzen ergeben sich aus dem US-Gesetz für hiesige IT-Abteilungen? Eines wird jedenfalls jetzt schon deutlich: Viele Bestimmungen von SOA dürften in unsere Corporate Governance Richtlinien einfliessen und damit auch im schweizerischen IT-Alltag bemerkbar werden. So verlangt eine der SOA-Bestimmungen die jährliche Prüfung der vom Management erstellten Berichte über die Wirksamkeit des internen Kontrollsystems. Eine Forderung, die so schon einigen CIOs schlaflose Nächte bereiten dürfte, wenn sie an die damit verbundenen administrativen Arbeiten und an neue Papierberge denken.

Doch was wird darüber hinaus geschehen? Findige IT-Auditoren werden umfangreiche Management-Letter verfassen, in denen dann zu lesen ist, dass die IT-Prozesse zwar wohl definiert sind, die Abläufe jedoch von den Mitarbeitern häufig nicht eingehalten werden. Ein ISO-Ordner im Schrank, das wissen wir schon lange, trägt kaum zur Prozesseffizienz und Produktequalität bei. Er stört aber auch nicht gross. Hat der praxisorientierte IT-Leiter nun wieder ein Problem mehr am Hals? Die strikte Überprüfung der vermeintlichen Bürokratie hindert ihn ja daran, kostengünstig zu arbeiten. Was lässt sich in dieser Situation tun?

a) Man ignoriert das ganze Kontrollgerede und hofft auf bessere Zeiten.

b) Man erlässt eine scharfe Weisung, die alles genau regelt, lässt jedoch durchblicken, dass im Einzelfall (in Notfällen und ab 23 Uhr) Kompromisse möglich sind.

c) Man macht aus der Not eine Tugend und definiert schlankere Prozesse mit wenigen aber wirksamen Kontrollmechanismen, und versucht diese auch gleich zu optimieren und, wo immer sinnvoll, zu automatisieren.

IT-Management oder IT-Chaos?

Doch wo beginnen? Es ist unglaublich: Während bei Produktionsbetrieben seit Jahren Qualitätsnormen und Standards gelten, kämpft die IT-Industrie noch immer wie mit Hellebarde und Armbrust gegen die täglichen Tücken der Technik. Jedem gewissenhaften IT-Auditor müssen sich die Haare sträuben! Schliesslich vergeht kaum ein Tag ohne peinliche Software-Panne oder öffentlichen Systemabsturz. Ein Blick in die Zeitung genügt: Da liest man von tausenden von Rekruten, die fälschlicherweise zum Dienst aufgeboten wurden, nur weil der Computer falsch gezählt hatte, oder man erfährt, dass Pendler ihr Lohngespräch verpasst haben, weil die SBB einen Ausfall im Computersystem hatten. Bisweilen geht das sogar so weit, dass bei Kantonsratswahlen Verlierer zu Gewinnern gemacht werden und umgekehrt – wie kürzlich in

St. Gallen geschehen. Im Einzelfall mag dies ja für die Betroffenen nur einfach ärgerlich sein. Aber fragen Sie einmal einen Wirtschaftsprüfer, der sich bei der Abschlussprüfung häufig auf genau solche IT-Systeme verlassen muss! Der weiss, dass sich auch in renommierten Unternehmen plötzlich riesige Bilanzlöcher auftun können, wenn bei der Datenaufbereitung irgendwo ein kleiner Fehler passiert. Das IT-Management kann sich nicht mehr lange hinter technischen Abkürzungen und einem für aussenstehende völlig undurchdringlichen Dschungel aus Software und Hardware verstecken. IT ist während der letzten Jahre definitiv zu einem überlebenswichtigen Faktor vieler Unternehmen geworden und benötigt wie die übrigen Abteilungen eines Unternehmens eine klare strategische Ausrichtung, professionelle Aufsicht und wirksame Kontrollen. Übrigens: Ob es auch mit IT-Problemen zu tun hat, wenn die Presse oft schon vor der Geschäftsleitung von Pleiten, Pech und Pannen Wind kriegt, bleibe für einmal dahingestellt.

Keine Hoffnung? COSO und COBIT bieten Hilfe!

Es ist oft nur ein scheinbarer Konflikt, der sich zwischen Kosteneffizienz und Kontrollmassnahmen abzuspielen scheint. SOA und Corporate Governance sind Realität. Leider gibt es noch zu viele Unternehmen, die ihren IT-Alltag ohne geeignete Strategie, ohne Risikoanalyse, und immer noch mit primitivsten manuellen Abläufen bewältigen – oder besser gesagt, von diesen überwältigt werden. Aber wenn sich die Technik laufend verändert, Systeme wachsen und komplexer werden, da gibt es nur eine Möglichkeit, die Fehlerquote halten oder gar reduzieren zu können: Das interne Kontrollsystem muss strategisch verankert und mit einer geeigneten Methodik konsequent ausgebaut und gelebt werden. Dazu wird auch hier in Europa zunehmend der COSO-Ansatz verfolgt – ein Konzept, das absolut SOA-konform ist und zur Steigerung der Effizienz im internen Controlling beitragen soll. COSO betrachtet das interne Kontrollsystem als integrierten Bestandteil der Geschäftsprozesse. Der Ansatz unterscheidet dabei folgende Zielbereiche: Strategy, Operations, Reporting und Compliance. Die ISACA hat sich intensiv mit den Implikationen von Corporate Governance auf die IT und die Rolle von IT-Prozessen im Finanzreporting auseinandergesetzt. Daraus ist COBIT entstanden – ein umfassendes Tool zur Umsetzung der SOA-Richtlinien im IT-Management.

Wenn in diesem Aufsatz auch nicht auf die Details eingegangen werden kann, so lohnt es sich doch, wenigstens die gravierendsten Schwachstellen zu kennen, die auch bei gut geführten IT-Abteilungen häufig vorzufinden sind.

Häufige Schwachstellen im IT-Management

Strategische Einbindung

COSO verlangt eine logische Verknüpfung zwischen Unternehmensstrategie, IT-Strategie und IT-Prozessen – ein Ansatz also, der für einen CIO enorme Chancen bietet und die IT-Abteilung zu einem Wachstumsmotor für das ganze Unternehmen machen kann. Leider lesen sich einige IT-Strategien wie technische Handbücher. Je nach Herkunft des CIO werden aktuelle Tools der Software-Entwicklung oder Highlights der Netzwerktopologie beleuchtet. Die wirklich wichtigen Aspekte wie die Definition der zu verwendenden Standards, Personal- und Ressourcenplanung, die Bestimmung einer langfristigen Technologie-Richtung und die Frage nach strategischen Partnerschaften kommen kaum je zur Sprache.

Auch die Risikoanalyse wird häufig vernachlässigt. Dabei kennt heute jeder „Murphy's Laws" und weiss, dass alles schiefgehen kann. Es schadet dem Unternehmen, wenn der CIO die Schwachstellen nur im Kopf hat oder in einer Schublade versteckt hält. Doch nicht nur der CEO, sondern auch der Verwaltungsrat, sollten jederzeit darüber aufgeklärt werden, wo die grössten Risiken liegen und welche Schwachstellen zu beseitigen sind.

Operations und Reporting

Während die Fachabteilungen immer stärker ausgeklügelte integrierte Systeme erhalten, kaum mehr etwas abtippen müssen und oft sogar Cut&Paste zu kompliziert ist, sieht es in manchen IT-Abteilungen bezüglich Ergonomie, Usability und Prozessdefinition noch aus wie in dunkler Vorzeit. Gegen die Tücken der Technik, Bug Reports und Change Requests wird in den meisten Fällen situativ und ohne geeignete Hilfsmittel gekämpft.

Aber ohne ein integriertes Workflow- und Planungssystem ist kaum ein effizientes Issue Tracking möglich. In der Not entwickelt dann der findige Programmierer schnell einmal eine bessere Pendenzenverwaltung, bastelt seine eigene Zeiterfassung oder macht sich gar an die Programmierung einer persönlichen Spesenabrechnung. Betrachtet man diese Entwicklungen aus einiger Distanz, kommt man unweigerlich zum Schluss: Von Integration keine Spur – Management: schwierig.

Vor den gleichen Problemen stehen auch die Projektleiter: Selten benötigte Formulare, Checklisten und Dokumente sind genau dann nicht auffindbar, wenn man sie braucht. Dabei gibt es heute bereits erprobte Lösungen, mit welchen ganze Formularsets (passende Ordnerrücken, Register, Standard-Traktandenlisten, Einladungen und Sitzungsprotokolle) vollautomatisch beim Projektstart generiert werden könnten. Auf Knopfdruck wäre die ganze Projektdokumentation in perfekter Corporate Identity für die gewünschte Anzahl von Projektmitgliedern erstellt – nur der Inhalt muss notabene noch selbst hinzugefügt werden.

Fehler bei Compliance

(Einhaltung von Gesetzen und Regulationen)

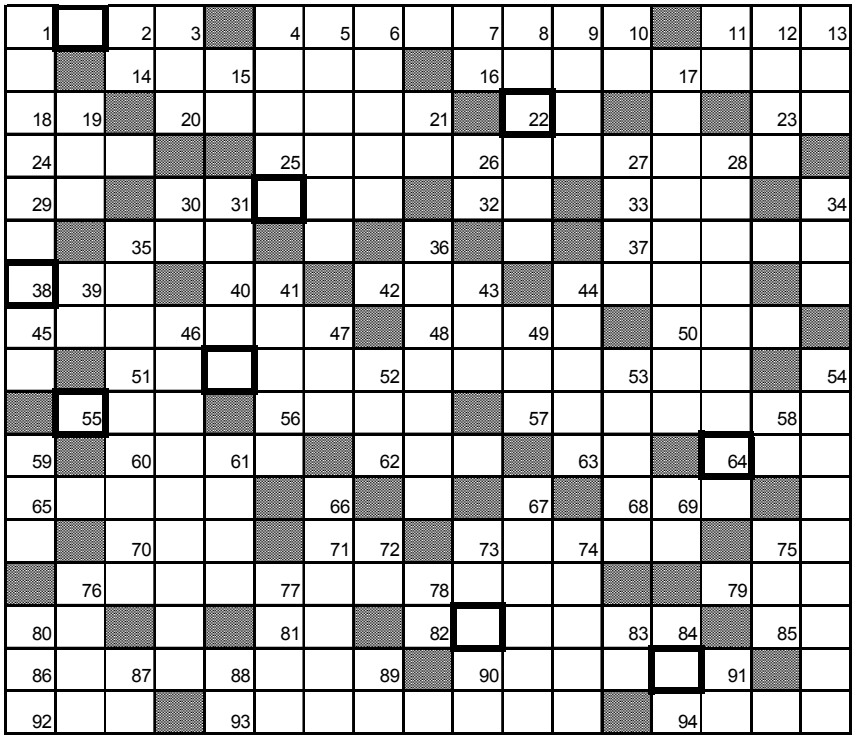
Die Anzahl neuer Gesetze und Verordnungen in Europa ist enorm. Wer nicht genau bestimmt, welcher Mitarbeiter diese durchzukämmen hat und wem die möglichen IT-Implikationen zu melden sind, könnte schon bald mit einem Bein im Gefängnis stehen. Compliance umfasst weit mehr als das Vermeiden von Interessenkonflikten, Geldwäscherei oder Korruption. Mittlerweile reicht das simple Einhalten formalrechtlicher Regelungen nicht mehr aus, um in der Öffentlichkeit einen glaubwürdigen Eindruck von Integrität zu präsentieren. Fortschrittliche Unternehmen entwickeln deshalb bereits zusätzliche unternehmensspezifische Verhaltensrichtlinien („Codes of Conduct“). Wie wichtig Compliance mittlerweile ist, zeigt auch, dass es sogar in der Schweiz bereits Ausbildungen zum Compliance-Spezialisten gibt.

Die Beschäftigung mit dem Sarbanes-Oxley-Act, COSO und COBIT lohnt sich also auch für Unternehmen, die nicht direkt vom US-Gesetz betroffen sind. Ein proaktiv handelnder CIO kann damit die Effizienz und Qualität des internen Kontrollsystems mit einem erprobten Konzept steigern und Schwachstellen in der IT frühzeitig erkennen.

Bruno Wenger,
Inhaber K&W Software AG

The ISACA Crossword Puzzle 3/04

Dieses Rätsel ist auf deutsch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.



Waagrecht: 1 Temperaturzustand; **4 via Radiowellen**; 11 Diener Mohammeds; 14 tankt man wohl nur in der Schweiz; 16 Gewässer ohne Abfluss (Mz); 18 zwei gleiche Konsonanten; 20 was der Donner tut; 22 französische AG; 23 CZ Zinn; 24 Lebensende; 25 greller Anstrich; 29 kurzes englisches Längenmass; 30 Platz für Pyramiden; 32 internationales Südost; 33 Fluss in Schottland; 35 siegen (E); 37 Attinghausens letztes Wort; 38 Kriemhilds Mutter; 40 F Adelsprädikat; 42 Wildwestmann (Wyatt); 44 Gesellin Oberons; 45 so ist der Propeller, wenn er läuft; 48 Heidis Betreuer; 50 so gut wie usw.; **51 darf nicht ausgelagert werden**; 55 allgemeine Zusatzversicherung (Abk); 56 Käsestadt; **57 Abgeschicktes**; 60 mit ver davor frostig, mit verr nicht da; 62 der Sage nach Hobby der Tahitianer; 63 niedrigster Offiziersrang (Abk), 64 hohe Spielklasse; 65 Körperpartie; 69 Mass in der Dynamik; 70 war einmal portugiesisch; 71 CZ Kupfer; 73 Titel (F); 75 AZ aus der Bundeshauptstadt; **76 heute sagt man forensic**; 79 Ham und Jaffet waren seine Brüder; 80 Gold (F); 81 Gespensterlaut; 82 Haushaltgerät; 85 Anschrift an Unbekannt; 86 24-karätiges Metall; 90 Gefäss; 92 drei gleiche Konsonanten; 93 Feldfrucht; 94 wenn nicht Wohnort der Layouterin, so doch eine Entschädigung.

Senkrecht: 1 Redeschwall; 2 Raummeter (Abk); 3 russischer Flugzeugtyp; 4 Bonbons; 5 Kleinmotorrad; 6 der Gott des Islam; 7 kurzer Tennisspieler; 8 Untugend; 9 nordischer Männername; 10 AZ aus der Innerschweiz; 11 Umlaut; 12 Weinernte; 14 Wasser aus der Schweiz zum schwarzen Meer; 15 AZ von ebenda; 17 so kann ein Beinahezusammenstoss sein; 19 Grundfarbe; 21 Technische Kommission; 26 römische Münze; 27 Stand; 28 mit Flüssigkeit versehen; 30 amerikanischer Soldat; 31 Asiat; 34 ich (L); **35 heute sagt man tools**; 36 Schlaginstrument; 39 Aufforderung zum machen; 41 auf der andern Seite (schweizerisch), 43 Schmiss; **46 Berufskollegin vieler Löser, wenn nicht selber**; 47 deutscher Kopfdenker (Abk); 49 in der Musik schon eher ein b; 52 Organisation Amerikanischer Staaten; 53 meistens geht auch der Wagenrücklauf; 54 ehelichte die schönste der Helleninnen; 58 AZ aus Holland; 59 Klostervorsteher; 61 rufen die italienischen Zuschauer beim Pferdesprung und beim Reckabgang; 66 Verpflichtung; **67 ohne Sorge**; 69 italienischer König; 72 erste Stufe der F Tonleiter; 73 Aufforderung an die Uhr zu laufen; 74 Merksatz; 75 der grosse steht in London; 76 Hänsels Schwester, wenn gross geworden; 77 Gesangsensemble; 78 tonloser spanischer Mehrzahlartikel; 80 nicht selten; 83 Rekrutenschule; 84 Aal (E); **87 unser Zentralthema**; 88 AZ

aus der Westschweiz; 89 kurzer Deckungsbeitrag 91 I Artikel.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, 8135 Langnau a/A. Lösungen werden auch entgegengenommen unter der e-mail-Adresse mbretscher@kpmg.com. Einsendeschluss ist der 20. August 2004.

If there are less than 5 answers, or the solution has not been found, the $US 50 go into the Watson Jackpot to be carried forward to the next issue. Watson: Each puzzle contains some anomaly that is to be detected. If correctly identified, the Watson Jackpot is broken and replenished with $US 50 for the next issue.

Solution Crossword Puzzle 2/04:
EUROCACS

Across: 1 *process*; 7 stola; 11 job; 14 EE; 15 lefty; 17 artery; 19 Nepal; 21 escrow; 24 trap; 25 l(ea)rn; 26 OP, 27 OTB; 30 L(ausanne) S(port); 31 un; 32 Joan; 34 BS; 35 eagle; 37 Susie; 38 noses; 40 tar; 41 astut(e); 43 CIA; 44 ta; 45 ardor; 46 rat; 48 garni; 50 SFM; 52 *executive*; 55 ASN; 56 timer; 57 tic; 58 vomit; 59 NE; 60 sic; 61 Toele; 63 été; 65 rasch; 67 Heiss; 68 Niger; 69 Al; 70 Riri; 71 OT; 72 TT; 74 non; 76 FC; 77 Lee; 79 Iqui(que); 82 Agassi; 84 lasso; 86 oblong; 88 Arian; 90 SE; 91 sou; 92 least; 93 *manager*.

Down: 1 Pen; 2 reel; 3 clan; 4 eel; 5 SF; 6 step; 8 tort; 9 law; 10 AR; 11 jerk; 12 ora; 13 bypass; 16 y(e)s; 18 TT; 20 programmes; 22 constructions; 23 *objectives*; 26 os; 28 *management*; 29 detest; 30 *leadership*; 31 UUU; 33 no; 34 beans; 36 Aa; 37 stretching; 39 strategies; 42 Sox (Sarbanes-Oxley); 47 at; 49 intern; 51 final; 53 ci; 54 vol; 52 Ost; 54 te; 65 radios; 66 CR; 72 EC; 73 Zulu; 75 oars; 76 firm; 77 Lana; 78 Esse; 80 QBO; 81 Io; 82 age; 83 sa; 84 LAN; 85 Oer; 87 NL; 89 IA.

Watson: In principle, there were two (intentional) Watsons. 1) all letters of the alphabet are used, 2) the letters of the solution are all in squares without numbers. Each one of them wins half of the jackpot. They were not detected.

There were less than 5 answers. The jackpot amounts to US$ 100.

Express Line

A Word from the Chair

On behalf of the Membership Board, I am pleased to congratulate the following chapters on their membership growth and retention efforts in 2003:

- Korea – Outstanding numeric growth
- Cochin – Outstanding percentage growth (175%)
- Papua New Guinea – Outstanding retention percentage (100%)
- Buenos Aires – Outstanding increase in retention (39%)

These awards will be presented at this year's leadership conferences.

Howard Nicholson
Chair, Membership Board

Certification Update

Both the CISA and CISM exams have attracted a record number of candidates for the 12 June 2004 exams.

For the 11th consecutive year, registration for the CISA exam has reached a new high. This year, more than 14,000 candidates have registered for the exam, which is an important step toward achieving the prestigious CISA designation. Such growth demonstrates the interest and importance of the CISA credential, which continues to attract information systems auditors in search of a practical certification that is globally respected and recognized.

In only its second year, nearly 700 candidates have registered for the CISM exam.

This new certification is on track to certify 5,000 professionals within its first two years.

ISACA International Headquarters thanks ISACA chapters for their considerable efforts in making the CISA and CISM exams so successful.

COBIT Online™ 3.1

COBIT Online's second release adds new functionalities for subscribers. The new release, 3.1, includes all the benefits and capabilities of the current COBIT Online, with the following additions:

- A community section, which provides a venue for users to ask and reply to questions and exchange experiences
- An expanded benchmark functionality
- Control practices, accessible via the Control Practices link when browsing the control objectives
- Print-screens with examples of all types of downloads in the functional overview
- New links to a glossary and a COBIT overview on the home page
- Integration of all help functions (FAQ, glossary, etc.) into one global, user-friendly Help function, available on each page
- Extra button at the control objective level that displays, in a pop-up window, the related statement from COBIT Quickstart (if there is a relation)

All these additions are designed to help users get more from their COBIT Online experience by expanding functionality, increasing ease of use, and enabling the sharing of experience and expertise.

DACH-News

CH:

euroCACS2004

Folgende Personen haben die ISACA Schweiz vor und während der euroCACS2004 in Zürich tatkräftig unterstützt und damit massgeblich zum guten Gelingen der Konferenz beigetragen.

Christine Schaller Felix
Marc Bucher
Bruno Wiederkehr
Michael Böni
Peter Bitterli
Cayhan Özgürol
Sukhwant Singh
Alois Marty
Christoph Meier
Tarik Oelmez
Fritz Kräuchi
Maher Kamal-Rizk
Martin Lutz
Radim Svejda
Felix Fehr
Christoph Oehri
Jean-Luc Nottaris
Reto Bürgi
Daniel Jörg
Felix Sutter

Im Namen des ganzen Vorstandes der ISACA Schweiz möchte ich den HelferInnen für Ihren Einsatz nochmals herzlich danken!

Chair euroCACS2004 Conference Partnering Chapter Committee

Thomas Bucher

CISA/CISM Club

Liebe CISA/CISMs

In der Vergangenheit wurden jeweils Besichtigungen organisiert (Telekurs, Kriminalmuseum). Wer würde an der Besichtigung des Fernsehstudios SRG SSR idée suisse in Zürich teilnehmen?

Termin Donnerstag, 4. November 2004, 17.30 h

Falls ich bis zum 31. September 2004 nicht zwölf Anmeldungen erhalte, werden ich die Führung absagen müssen.

thomas.bucher@ch.ey.com

CISA/CISM-Koordinator
Thomas Bucher

News aus den Interessengruppen

IG Operational IT-Risk/Basel II

Neu!

Peter R. Bitterli
Bitterli Consulting AG
Konradstrasse 1
8005 Zürich
Tel. + 41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

Interessenten melden sich bitte bei Peter R. Bitterli

IG Government IT-Audit („Closed user group“)

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Programme 2004 :
Les séances suivantes auront lieu les 24.8.2004 et 16.11.2004.

La participation à ce groupe est réservée aux collaborateurs des organes de contrôle.

IG Computer Forensics

Nouveau!

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe-Motta 50
1211 Geneva 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
Mobile: +41 79 220 54 07
Paul.Wang@ch.pwc.com

L’objectif de ce groupe de discussion lié aux « Computer Forensics », est de fournir un forum d’intérêt et d’information sur les méthodologies et les outils de ce qu’on appelle communément en français « Assistance informatico-légale » Ce forum offre la possibilité de partager des idées, des technologies, des outils et certainement aussi des notions juridiques de ce domaine en constante évolution. Ce groupe de discussion abordera également des discussions techniques et procédurales sur les prérequis en matière de recherche de preuves informatiques. Même si les participants doivent être familiers avec la recherche, l’acquisition et l’analyse de preuves informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT-Governance

Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@ch.ey.com

Letzte Sitzung: Kick-off Sitzung am 4. März 2004, bei Ernst & Young AG, Zürich

Nächste Sitzung: Die für den 6. Mai 2004 vorgesehene Sitzung musste leider verschoben werden. Es wird ein neuer Termin festgelegt.

Traktanden:
- Präsentation der beiden Pilotprozesse PO1 und PO10
- Festlegen weiteres Vorgehen

IG Romandie

Vacant : touts personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s’annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

IG Outsourcing/Insourcing

Ulrich Engler
Swiss Life
CF/REV HG 3151
General-Guisan-Quai 40
Postfach, 8022 Zürich
Telefon +41 43 284 77 58
Telefax +41 43 284 47 33
ulrich.engler@swisslife.ch

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Mögliche Themen: Kontiniuität des Insourcers, Abhängigkeit vom Insourcer (Konkurs), Überarbeitetes Rundschreiben EBK, Fernwartung, etc.

Geplant sind *Gespräche* zum Thema „Grounding“ eines IT Service Providers mit ausgewählten Gesprächspartnern aus den Bereichen Legal, Service Provider, Industrie und Financial Services.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@ch.ey.com

Letzte Sitzung: Freitag, 16. Januar 2004, bei Ernst & Young AG, Zürich

Traktanden:

- Referenzmodell Data Load
- Risk Matrix
- Fact Sheets

Nächste Sitzungen: Für Informationen melden Sie sich bitte bei Daniel Oser.

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijoustrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Letzte Sitzung: Donnerstag, 13. Mai 2003

Nächste Sitzung: Gemäss Protokoll der Sitzung vom 13. Mai 2004

Ein Revisor, der trank auf Schloss Laufen 'nen Roten
Beim Fackelzug, da verbrannte er tüchtig die Pfoten,
Der Alkohol gab ihm den schrecklichen Einfall,
Die ISACA sei neulich zu finden am Rheinfall,
Die Konferenz, wie wir wissen, war aber in Kloten.

In Zurich, the ISACA held one of its conferences,
Several participants made terrible inferences:
Whilst it was clear that the airport was loud,
It possibly would provide for a ride on a cloud,
But doing so, they lost all the cores and their competences.

Veranstaltungen

Intensivlehrgang für Informations- und Sicherheitsbeauftragte	14.–18. Juni 2004 Zürich, 5 Tage, Infosec
Security Briefing	16. Juni 2004 Zug, 1 Tag, InfoGuard
BS7799 Implementation	16.–18. Juni 2004 Zürich, 3 Tage, InfoGuard
Auditorenkurs nach BS7799	21.–25. Juni 2004 Zürich, 5 Tage, Infosec
IT Risk Management (After Hour Seminar im Landesmuseum)	30. Juni 2004 Zürich, ISACA CH
Securing and Auditing Windows 2000 Server	6.–9. Juli 2004 London, 4 Tage, MIS
The ISI Network Infrastructure Security Academy	2.–13. August 2004 London, 10 Tage, MIS
Oracle Training Week	16.–20. August 2004 Genève, 5 Tage, MIS
SAP R/3 – Workshop „Grundlagen“ für Wirtschafts- und Informatikprüfer	17.–20. August 2004 Stuttgart, 4 Tage, ISACA CH
SAP R/3 – Workshop „Prüfung von Geschäftsprozessen“ für Wirtschafts- und Informatikprüfer	23.–25. August 2004 Stuttgart, 3 Tage, ISACA CH
IIT Self Assessment am Europäischen Rechnungshof (After Hour Seminar im Landesmuseum)	25. August 2004 Zürich, ISACA CH
Evidence Lab – Workshop über die Spurensuche in Computersystemen	30. August – 1. September 2004 Zürich, 3 Tage, ISACA CH
Thema noch offen: siehe www.isaca.ch (After Hour Seminar im Landesmuseum)	2. September 2004 Zürich, ISACA CH
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	7.–9. September 2004 Zürich, 3 Tage, ISACA CH
Zweite deutsche IT Governance Konferenz 2004	13./14. September 2004 Berlin, 2 Tage, ISACA/marcevans
PRINCE2 – Planung und Organisation mit flexibler Projektmanagement-Methode	21.–23. September 2004 **(Neu)** Zürich, 3 Tage, ISACA CH
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	28.–30. September 2004 Zürich, 3 Tage, ISACA CH
Sarbanes-Oxley – A Road Map top Compliance	7./8. Oktober 2004 London, 2 Tage, MIS
Thema noch offen: siehe www.isaca.ch (After Hour Seminar im Landesmuseum)	20. Oktober 2004 Zürich, ISACA CH

Kontaktadressen Veranstalter

Der *NewsLetter* empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
Tel. +33 1 55 62 12 22
afai@afai.asso.fr
www.afai.asso.fr

advanced technology seminars
Grundgasse 13
CH-9500 Wil
Tel. +41 71 911 99 15
Fax. +41 71 911 99 16
Maurer@inf.ethz.ch

Stiftung für Datenschutz und Informationssicherheit
Dr. Beat Rudin
Kirschgartenstrasse 7
Postfach
CH-4010 Basel
Tel. +41 61 270 17 70
Fax +41 61 270 17 71
beat.rudin@privacy-security.ch
www.privacy-security.ch

e-tec Security
PO Box 54
Wilmslow Chesire SK9 6FU
United Kingdom
info@a-tecsecurity.com

Euroform Deutschland GmbH
Hans-Günther-Sohl-Strasse 7
D-40235 Düsseldorf
Tel. +49 211 96 86 300
Fax. +49 211 96 86 509
info@euroforum.com

Hochschule für Technik Rapperswil
Institut für Internet Technologien und Anwendungen
Oberseestrasse 10
8640 Rapperwil
Tel. +41 55 222 41 11
Fax. +41 55 222 44 00
office@hsr.ch

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@iir-ev.de

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Tel. +41 41 749 19 00
Fax +41 41 749 19 10
www.infosec.com

Integralis GmbH
Gutenbergstr. 1
D-85737 Ismaning
Tel. +49 89 94573 447
Fax +49 89 94573 199 fx
schulung@integralis.de

ISACA CH
Kurssekretariat
c/o. ITACS Training AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 64
Fax. +41 1 440 33 61
kurse@isaca.ch

ISACA USA
3701 Algonquin Rd #1010
USA_Rolling Meadows IL 60008
Tel. +1 847 253 15 45
Fax. +1 847 253 14 43
www.isaca.org

Marcus Evans
Weteringschans 109
1017 SB, Amsterdam
The Netherlands
Tel. +31 20 531 28 13
Fax. +31 20 428 96 24
www.marcusevansnl.com

MIS Training Institute
Nestor House
Playhouse Yard P.O. Box 21
GB-London EC4V 5EX
Tel. +44 171 779 8944
Fax. +44 171 779 8293
www.misti.com

MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Tel. +41 1 360 70 70
Fax. +41 1 360 77 77
it@mediasec.ch

Secorvo Security Consulting GmbH
Secorvo College
Albert-Nestler-Strasse 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
info@secorvo.de
www.secorvo.de

Treuhand-Kammer
Jungholzstrasse 43
Postfach
CH-8050 Zürich
Tel. +41 1 305 38 60
Fax. + 41 1 305 38 61

ZfU Zentrum für Unternehmensführung AG
Im Park 4
CH-8800 Thalwil
Tel. +41 1 720 88 88
Fax. +41 720 08 88
info@zfu.c

Germany Chapter

Vereinsadressen

Geschäftsstelle
ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
Fax. +49 2064 733192
isaca.dinslaken@t-online.de

Präsidentin
Karin Thelemann
Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 10–12
65760 Eschborn/Frankfurt am Main
Tel. +49 6196 99626 488
Fax. +49 6196 99626 449
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
KPMG
Marie-Curie-Str. 30
D-60439 Frankfurt
Tel. +49 69 9587 2313
Fax. +49 69 9587 192313
MarkusGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
PwC Deutsche Revision AG
Friedrich-List-Str. 20
D-45128 Essen
Tel. +49 201 438 0
Fax. +49 201 438 1000
Norbert.Groening@
de.pwcglobal.com

Public Relations
Heinrich Geis
Deutsche Börse AG
Neue Börsenstrasse 1
D-60487 Frankfurt
Tel. +49 692 101 5149
Fax. +49 692 101 4396
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
WLSGV-Prüfungsstelle
Regina-Portmann-Strasse 1
D-48159 Münster/Westfalen
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
comdirect private finance AG
Pascalkehre 15
25451 Quickborn
Tel. +49 4106 704 2336
Fax. +49 4106 704 2301
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Michael M. Schneider
Deloitte & Touche
Schumannstraße 27
60325 Frankfurt am Main
Tel. +49-69 75606 121
Fax. +49-69 75695 84448
michaelschneider@deloitte.de

Austria Chapter

Vereinsadressen

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand, CIA, WP, StB
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2831
michael.schirmbrand@at.eyi.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Österreichische Kontrollbank Aktiengesellschaft
Strauchgasse 1–3
1010 Wien
Tel: +43 1 531 27-857
maria-theresia.stadler@oekb.co.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner, StB
GRT Price Waterhouse
Prinz-Eugen-Straße 72
1040 Wien
Tel: +43 1 50188-0

Sekretär
Mag. Gunther Reimoser, CISA
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 21170-4113
gunther.reimoser@at.eyi.com

Kassier
Mag. Helmut Zodl
IBM Österreich
Obere Donaustraße 95
1020 Wien
Tel: +43 1 21145-0
helmut_zodl@at.ibm.com

CISA-Koordinatorin
Mag. Maria Rieder
Münze Österreich AG
Am Heumarkt 1
1010 Wien
Tel: +43 1 71715-0
maria.rieder@aon.at

Public Relations/Newsletter-Koordination
Rolf von Rössing
MA, D.E.s.s, CBCP, MBCI
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2812
dk@cos-ag.de

E-Mail ISACA Austria Chapter:
office@isaca.at
Homepage ISACA Austria Chapter:
www.isaca.at

Switzerland Chapter

Vereinsadressen

Präsidentin
Daniela S. Gschwend
Swiss Re
Mythenquai 50/60
8022 Zürich
Tel. +41 43 285 69 36
Fax. +41 43 285 33 69
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Thurgauer Kantonalbank
Bankplatz 1
8570 Weinfelden
Tel. +41 71 626 64 61
Fax. +41 71 626 63 60
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Ernst & Young AG
Postfach
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 40 14
thomas.bucher@ch.ey.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4022 Basel
Tel. +41 61 697 72 41
Fax. +41 61 697 78 44
monika.josi@ah.novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe Motta 50
1211 Genève 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
paul.wang@ch.pwcglobal.com

Marketing
Bruno Wiederkehr
ICT Consulting & Training
Rigistrasse 3
CH-8703 Erlenbach
Tel. +41 1 910 96 33
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch