Information Systems Audit and Control Association

News Letter

Nr. 62, Februar 2003

Thema Datenschutz

Switzerland Chapter
Germany Chapter
Austria Chapter

© 3.2.2003

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
PricewaterhouseCoopers AG
Nordstrasse 15
8035 Zürich

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: 1000 Exemplare

Nächste Ausgabe (Thema: Datenschutz Fortsetzung): April 2003, Redaktionsschluss: 1. April 2003

Inhaltsverzeichnis

Editorial 4

Datenschutz – La modernisation de la protection des données et le rôle du Préposé fédéral à la protection des données 5

Datenschutz – Datenschutz in Unternehmen: Intern oder outgesourced 8

Datenschutz – Datenschutz im internationalen Unternehmensverbund 11

Datenschutz – La protection des données : pourquoi et comment ? 16

CISM – Braucht unsere Gesellschaft den neuen Titel? 20

CISM – Le CISM, une combinaision gagnante 21

Express Line 23

The ISACA Crossword Puzzle 24

News aus den Interessengruppen 25

DACH-News 27

Veranstaltungen 29

Germany Chapter 31

Austria Chapter 32

Switzerland Chapter 33

Editorial

Es gab einmal eine Zeit, da war „jedermann“ darauf bedacht, einen guten Ruf zu haben. Man war stolz darauf und konnte die Information nicht genug breit streuen. Und dann kam der Datenschutz.

Plötzlich schien die Welt auf dem Kopf zu stehen: Ich kann mir den Eindruck nicht verwehren, dass der Anschein vorherrscht, „jedermann“ sei nun darauf bedacht, dass niemand etwas über seinen schlechten Ruf erfährt. Als ehemaliger Datenschutzbeauftragter eines Rechenzentrums nach deutschem Datenschutzgesetz nahm ich an verschiedenen Tagungen teil und konnte diesen Eindruck nie loswerden. Niemand konnte mir bis heute überzeugend und eindeutig belegen, dass mein Eindruck falsch sei. Häufig wurde mir klar gemacht, dass ich eben den Gedanken des Datenschutzes nicht verstehe. Und dabei blieb es.

Worum geht es überhaupt? Die einen argumentieren, Datenschutz sei Privatsache; wieder andere, es sei Ansichtsache. Die verschiedenen Länder kennen unterschiedliche Interpretationen des Begriffs, der betroffenen Personen und der Unterlagen.

Das Feld der Informatik-Revision ist direkt betroffen. Sehr oft wird argumentiert, die Informatik begünstige Verletzungen des Datenschutzgedankens. Die erste Version des französischen Datenschutzgesetzes beschränkte sich wohl deshalb auf elektronisch gespeicherte Daten. Wo sich das deutsche Datenschutzgesetz in seiner ersten Version auf Daten bezüglich natürlicher Personen beschränkte, schloss das schweizerische gleich auch die juristischen Personen in den Kreis der schutzwürdigen „Objekte“ ein. Was gilt?

Natürlich kann ich mich mit dem Gedanken befreunden, dass jedermann ein Recht auf seine Privatsphäre haben soll. Auch glaube ich, das Wesen des schweizerischen Bankgeheimnisses, der Berufs- und Geschäftsgeheimnisse zu kennen. Aber wird mit dem Schlagwort „Datenschutz“ eben nicht allzu oft Schindluderei getrieben und fordern nicht häufig Gesetzgeber sowie angeblich Betroffene kommunikationsbehindernde Massnahmen?!

Diese Ausgabe des *NewsLetters* versucht, etwas Licht in den Nebel des Datenschutzverständnisses zu bringen, indem u.a. dargelegt wird, wie die verschiedenen Instanzen mit der Thematik umgehen. Ich wünsche den Lesern viel Spass und Erleuchtung.

Max F. Bretscher, Redaktor

Il y a bien longtemps, « chacun » s’efforçait d’avoir une bonne réputation. On était fier de cette image et tous les moyens étaient bon pour la diffuser le plus largement possible. Puis vint la protection des données…

Le monde sembla soudainment bouleversé. J’ai de la peine à m’enlever l’idée de la tête que depuis, « chacun » s’efforce surtout de faire en sorte que personne n’apprenne qu’il a mauvaise réputation. J’ai participé en qualité de chargé de la protection des données d’un centre de calcul (selon la législation allemande) à de nombreuses conférences et je n’ai pas réussi à me débarrasser de cette idée. Des spécialistes ont essayé sans succès de me convaincre. Ils ont conclu que je n’avait pas saisi le sens profond de la protection des données. Et on en resta là.

Mais de quoi parle-t-on en fait ? Certains affirment que la protection des données est une affaire privée, pour d’autres une question de point de vue. Chaque pays diffère dans son interprétation des notions, dans le cercle des personnes et la définition des documents à protéger.

L’audit informatique est souvent directement mis en cause. On lui reproche notamment de couvrir de graves atteintes à la protection des données. Une des raisons qui a conduit la première mouture de la législation française sur la protection des données à se concentrer sur les données enregistrées sous forme électronique. Divergences également entre la première législation allemande sur la protection des données qui se limitait aux personnes physi-

ques, alors que la législation suisse inclue également les personnes morales dans le cercle de protection. Où se situe la vérité ?

Je suis bien sûr acquis à l'idée que chacun à droit à une sphère privée protégée. Je crois également bien connaître le secret bancaire suisse et les secrets professionnel et de fonction. Mais le concept de « protection des données » n'est-il pas aujourd'hui détourné de son but premier pour couvrir des comportements absurdes et promouvoir des mesures législatives qui entravent la communication ?

Ce numéro de votre *NewsLetter* tente d'apporter un peu de lumière dans le brouillard de la protection des données en permettant notamment aux différentes instances de présenter leur point de vue. Je vous souhaite, chers lecteurs, une bonne et instructive lecture.

Max F. Bretscher, Rédacteur

Datenschutz

La modernisation de la protection des données et le rôle du Préposé fédéral à la protection des données

Introduction

La loi fédérale sur la protection des données a 10 ans. C'est le moment que le Conseil fédéral a choisi pour effectuer une révision partielle de la LPD. Début 2003, il va adresser un message en ce sens au Parlement. Cette révision fait suite à deux motions parlementaires visant à renforcer la protection des données dans le cadre des liaisons en ligne et à la transparence lors de la collecte des données personnelles. Cette révision doit également permettre à la Suisse de ratifier le protocole additionnel à la Convention du Conseil de l'Europe à l'égard du traitement automatisé des données à caractère personnel. Ce protocole concerne les autorités de contrôle et les flux transfrontières données. Même si la révision permet un rapprochement avec le droit européen et la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, elle ne constitue pas une loi de transposition de la dite directive. Si les négociations bilatérales II entre la Suisse et l'Union européenne aboutissent, une révision plus substantielle de la loi sera nécessaire pour mettre notre droit en parfaite harmonie avec les exigences européennes, la directive faisant partie de l'acquis communautaire que la Suisse serait appelé à reprendre.

Révision de la loi fédérale sur la protection des données

Le projet de révision renforce la position des personnes concernées, notamment en introduisant une obligation de transparence lors de la collecte de données personnelles. Toute collecte de données devra à l'avenir être reconnaissable pour la personne concernée et faire l'objet d'une information active de la part des responsables du traitement lorsqu'elle concerne des données sensibles ou des profils de la personnalité. Dans le secteur privé, le droit de s'opposer à un traitement sera rendu plus effectif, notamment en incitant le responsable du traitement à se déterminer lors d'une requête d'un individu. Le régime des flux transfrontières de données sera revu. D'une part le système de la déclaration préalable sera abandonné, d'autre part tout en maintenant le système de l'interdiction de transfert lorsque la personnalité des personnes concernées est gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection des données adéquat, la loi aménagera des dérogations à cette

interdiction (recours à des clauses contractuelles de protection des données, règlement de protection des données pour les groupements d'entreprise). L'annonce des fichiers est maintenue tant pour les organes fédéraux que pour les personnes privées. Toutefois, des dérogations à l'annonce seront introduites dans la loi et la procédure d'annonce sera simplifiée, notamment par l'introduction, dans un avenir proche, de la possibilité pour le maître de fichier de déclarer ses fichiers en ligne. S'inspirant de la loi sur l'environnement et du droit allemand de la protection des données, il est également prévu d'encourager le recours à la certification des produits et des systèmes de traitement des données personnelles (audit, label de qualité de protection des données).

Procédure de certification (audit)

La certification de protection des données est un encouragement au responsable de traitement de recourir, volontairement, à une procédure qui doit contribuer à une amélioration constante de la protection des données. L'entreprise ou l'organe étatique qui se soumet à une telle procédure d'audit y trouve également un avantage en pouvant afficher une image de conformité aux exigences de la protection des données. Dans un monde globalisé où les échanges d'informations se sont banalisées, la protection des données revêt un caractère indispensable et devient un facteur de confiance et d'acceptation, notamment dans la perspective du commerce électronique ou de l'administration en ligne. Une protection des données effective devient ainsi également un avantage concurrentiel.

L'audit de protection des données permet de renforcer la responsabilité individuelle et de stimuler la concurrence. Il favorise une amélioration continue de la protection et de la sécurité des données et établit un système d'apprentissage permanent. La certification et l'attribution d'un label de qualité « protection des données » impliquent que les exigences légales de la protection des données soient prises en considération dans le développement des systèmes de traitements de données sous l'angle technique et organisationnel, à savoir que ces exigences soient appliquées à l'aide de normes techniques. L'effectivité du label de qualité repose sur le respect de différents critères et notamment :

- la procédure de certification et le processus d'attribution du label doivent être transparents et se baser sur des critères reconnus au plan international ;
- les critères d'évaluation doivent être clairement définis et fixés par des normes correspondant aux exigences légales ;
- le label doit être délivré par une institution agréée et qualifiée dans le cadre d'une procédure d'audit.

Avant qu'un label de qualité de protection des données ne soit attribué, il convient de s'assurer dans le cadre de la procédure d'audit que le traitement de données personnelles se fasse conformément aux exigences légales. Le Préposé fédéral à la protection des données (PFPD) dans son 8e rapport d'activités a fixé les exigences qui doivent être vérifiées :

- la garantie d'une information transparente à l'utilisateur ou au client, notamment en développant et en publiant une politique de respect de la vie privée ;
- le respect des exigences légales applicables au traitement de données et notamment l'existence d'un motif justificatif légitimant le traitement et de critères régissant la mise à jour, la conservation, l'effacement et la transmission des données personnelles ;
- les garanties relatives à l'exercice des droits des personnes concernées et en particulier le droit d'accès et de rectification ;
- la possibilité pour l'utilisateur ou le client de choisir s'il souhaite ou non que ses données soient utilisées,
- les mesures techniques et organisationnelles pour assurer la sécurité des données.

L'octroi d'un label de qualité de protection des données ne constitue en aucun cas un acquis définitif. Il est nécessaire de procéder ultérieurement et régulièrement à des contrôles (internes et externes). Ces contrôles doivent reposer sur un processus sûr et être effectués par des organes indépendants et compétents en matière de contrôle. Si les dispositions et les exigences légales de protection des données ne sont pas respectées, des mesures ou des sanctions doivent être prises. Elles peuvent aller jusqu'au retrait du label de qualité.

La certification et l'attribution de labels de qualité doivent en principe demeurer en mains des entreprises privées. Le législateur devra se contenter d'édicter des prescriptions sur la reconnaissance des procédures de certification et sur l'introduction du

label. Les organes de certification pourraient être soumis à une obligation d'accréditation et les labels attribués faire l'objet d'une publicité. Il devrait à cet effet tenir compte du droit international et des normes techniques reconnues au niveau international. Le PFPD ne devrait pas être une instance de certification ou d'attribution des labels. Par contre, il devrait pouvoir examiner les méthodes utilisées pour procéder à la certification et le cas échéant émettre des recommandations (révision de protection des données). Dans le cadre de ses compétences, il pourra le cas échéant non seulement s'assurer que les entreprises certifiées respectent les exigences de protection des données, mais également que les entreprises qui évaluent, le font conformément aux exigences de la protection des données.

La certification et l'attribution de labels de qualité de protection des données constituent une mesure de l'auto responsabilisation des responsables de traitement. D'autres mesures pourraient encore être envisagées et par exemple l'encouragement à utiliser des technologies de la vie privée et l'adoption de codes sectoriels de conduite.

Les compétences du PFPD

L'action des autorités de protection des données et notamment du PFPD doit s'attacher à sensibiliser les personnes concernées et les responsables de traitement aux risques liés au traitement des données personnelles. Cela implique en particulier une politique d'information active, une évaluation des risques et l'élaboration, en concertation avec les milieux concernés, d'« outils » pour permettre de réaliser les exigences de la protection des données et diminuer les risques d'atteinte aux droits des personnes concernées, ainsi que le contrôle des exigences légales.

L'effectivité de la protection des données dépend aussi du rôle et des compétences des autorités de surveillance, tel que le PFPD. Une plus grande responsabilisation des maîtres de fichiers doit avoir ainsi pour conséquence la mise en place de moyens de contrôle préventifs et répressifs en cas d'abus. Cela implique qu'à l'avenir, les autorités de surveillance ait un rôle plus pro-actif. L'objectif des autorités de protection des données est d'éviter que les individus se trouvent dépourvus de toute protection lorsque des données les concernant font l'objet de traitements. Cet objectif n'est par contre pas d'empêcher les traitements de données. Il est nécessaire de développer une politique qui promeut la reconnaissance et le respect des principes de la protection des données et qui permet aux personnes concernées d'exercer effectivement leurs droits. Le rôle des autorités de surveillance est dès lors de veiller à ce que ces règles soient respectées et intégrées dans les processus de traitements des données et les systèmes d'informations, notamment en favorisant le recours aux technologies pour intégrer les principes de base de la protection des données.

Par contre, le PFPD doit non seulement contrôler le respect des exigences légales. En cas de violation de ces exigences, il doit aussi pouvoir prendre les mesures adéquates qui s'imposent et le cas échéant prononcer des sanctions. L'effectivité de la surveillance nécessite des ressources, qui aujourd'hui sont insuffisantes, et des pouvoirs de décision. A l'instar d'autres autorités de protection des données en Europe et d'autres autorités de surveillance en Suisse, par ex. la commission fédérale de la concurrence, il serait souhaitable que le PFPD soit également doté du pouvoir de prononcer des sanctions.

Jean-Philippe Walter, Dr. en droit, Préposé fédéral suppléant à la protection des données, Berne

Datenschutz

Datenschutz in Unternehmen: Intern oder outgesourced

Anforderung, Aufgaben und rechtliche Grundlagen für Datenschutzbeauftragte

War Datenschutz in vielen Unternehmen lange Zeit ein stiefmütterlich behandeltes Thema, hat sich dies durch die zunehmende Automatisierung vieler Geschäftsprozesse geändert. Längst haben wir uns daran gewöhnt, dass personenbezogene Daten[1] elektronisch gespeichert und genutzt werden. Seit New Economy und e-business gehört der Austausch personenbezogener Daten über Unternehmensgrenzen hinweg zum Alltäglichen[2]. Die öffentliche Diskussion der meist internetbasierten neuen Geschäftsmodelle hat jedoch Kunden und Lieferanten beim Thema Datenschutz sensibler werden lassen. Unternehmen, die personenbezogene Daten verarbeiten, sind daher heute mit strengeren Regeln konfrontiert als früher. Datenschutz „auf Sparflamme“ ist nicht mehr möglich.

Um den gestiegenen Anforderungen und Regelungen des Datenschutzes effektiv gerecht zu werden, stellt sich für Unternehmen die Frage, ob sie weiter in internes Wissen investieren oder ob sie die Tätigkeit des Datenschutzbeauftragten (im Folgenden DSB genannt) ganz bzw. teilweise an Spezialisten auslagern sollten.
Im Folgenden werden die Grundlagen, zu beachtende Besonderheiten beim Outsourcen des DSB sowie das Für und Wider dargestellt.

Die Bestellung des DSB – wann ist sie notwendig?

Unternehmen müssen unter verschiedenen Voraussetzungen einen Datenschutzbeauftragten bestimmen: Gemäß des deutschen Datenschutzgesetzes § 4f Abs.1 BDSG muss innerhalb eines Monats ein DSB beauftragt werden, wenn

- das Unternehmen personenbezogene Daten automatisiert erhebt, verarbeitet oder nutzt und mehr als vier Personen hiermit beschäftigt,
- das Unternehmen personenbezogene Daten nicht automatisiert erhebt, verarbeit oder nutzt, sondern für diese Aufgaben mindestens 20 Personen beschäftigt.

Diese Größenvoraussetzungen werden von mittelständischen Unternehmen regelmäßig erfüllt. Unabhängig von der Zahl der mit dem Erheben, Verarbeiten oder Nutzen personenbezogener Daten beschäftigter Arbeitnehmer müssen Unternehmen einen DSB beauftragen, wenn Sie Verfahren einsetzen, die der Vorabkontrolle (vgl. § 4d Abs. 5 u. 6 BDSG) unterliegen. Das betrifft Verfahren, die besonders sensible Daten verarbeiten oder zur Beurteilung von Personen dienen.

Organisationsformen des DSB

Für den DSB bieten sich vier unterschiedliche Organisationsformen an:

- Interner DSB: Hierfür wird ein Mitarbeiter benannt, der direkt dem Vorstand bzw. der Geschäftsführung berichtet. Idealerweise bestellt das Unternehmen den DSB hauptamtlich, um Interessenkollisionen zu vermeiden.
- Interner DSB mit externer Unterstützung: Der zum DSB ernannte Mitarbeiter erhält fallweise Unterstützung durch einen externen Dienstleister, z. B. in Zweifelsfragen oder bei Projekten.
- Externer DSB: Eine unternehmensexterne Person übernimmt die Funktion des DSB.
- „Konzerndatenschutz-Beauftragter“: Ein sogenannter Konzerndatenschutzbeauftragter ist i. d. R. ein interner DSB bei einem Unternehmen eines Konzerns – z. B. der Konzernmutter. Gleichzeitig ist er externer Datenschutzbeauftragter bei den übrigen Konzernunternehmen. Möchten einzelne Konzernunternehmen ihren bisherigen DSB beibehalten oder ist der gesamte Konzern zu groß für einen einzelnen DSB, bietet es sich an, den Konzerndatenschutzbeauftragten als Koordinator einzusetzen. Bei jeder Art der Organisation des Konzerndatenschutzbeauftragten kann ein externer Dienstleister die Tätigkeit entweder vollständig übernehmen oder unterstützend wirken.

Rechtliche Grundlage für die Beauftragung eines externen DSB

Anforderungen: juristische und technische Expertise

Generell schreibt das BDSG in § 4f Abs. 2 vor, dass der DSB fachkundig und zuverlässig sein muss. Know-how muss der DSB auf mehreren Bereichen mitbringen: Immer anspruchsvoller werden die IT-Technologien, die zur Verarbeitung und Nutzung personenbezogener Daten eingesetzt werden. So muss ein DSB beispielsweise im Detail die technischen Schritte beim Profiling verstehen, wenn er ein solches Verfahren beurteilen möchte. Angesichts des komplexen EDV-Rechtes braucht der DSB außer solchen technischen Qualifikationen auch ein juristisches Verständnis der Dinge. De facto sind jedoch die „eierlegenden Wollmilchsäue", die alle juristischen und technischen Anforderungen erfüllen, kaum zu bekommen. Ein nur scheinbarer Ausweg ist es, dem DSB als fachliche Unterstützung verschiedene unternehmenseigene Spezialisten als Gehilfen zur Seite zu stellen, denn die primären Aufgaben dieser Gehilfen können sich als unvereinbar mit den Interessen des Personendatenschutzes erweisen. Davon abgesehen sind interne Mitarbeiter aber meist ohnehin hochgradig ausgelastet und letztlich wird ihre eigene Arbeit eine höhere Priorität haben als der Personendatenschutz.

Die Möglichkeit des Outsourcens

Angesichts der erläuterten Fakten ist es in vielen Fällen sinnvoller, einen externen DSB zu bestellen. Ein großer Vorteil ist etwa, dass der ausgelagerte DSB eine Dachorganisation im Rücken hat, die über entsprechende fachliche und personelle Ressourcen verfügt. Das Gesetz regelt die Möglichkeit den DSB auszulagern explizit in § 4f Abs. 2 BDSG: „Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden."

Zu beachten ist dabei, dass als DSB nur eine natürliche Person, nicht aber ein Unternehmen (juristische Person) bestellt werden kann.

Wer kommt in Betracht?

Aufgrund der erforderlichen Fachkunde und Zuverlässigkeit des DSB kommt nur ein beschränkter Personenkreis für die Tätigkeit als externer DSB in Betracht[3]. Dies sind etwa Personen mit Erfahrung in IT-Prüfungen im Rahmen von Jahresabschlussprüfungen oder Sonderprüfungen. Besonders geeignete Anwärter sind daher z. B. Träger eines CISA-Titels[4], wenn sie durch Rechtsanwälte einer nahestehenden Kanzlei, in juristischen Fragestellungen unterstützt werden.

Geeignete DSB sind auch Rechtsanwälte, Wirtschaftsprüfer und Steuerberater. Des weiteren können Unternehmensberater, Mitarbeiter von Datenschutz-Serviceunternehmen, Mitarbeiter von Interessenverbänden und berufsständischen Vereinigungen sowie Mitarbeiter eines für das Unternehmen tätigen Service-Rechenzentrums als DSB fungieren. Zu beachten ist dabei jedoch, dass der DSB nicht gegen den Grundsatz der Unabhängigkeit bei der Prüfung von IT-Prozessen verstoßen darf[5].

Wirtschaftlichkeitsbetrachtung: Externer oder interner DSB?

Während sich die Kosten des externen DSB leicht beziffern lassen, sind die Opportunitätsverluste des internen DSB nicht ohne weiteres zu ermitteln. Ein fairer Vergleich zwischen der Wirtschaftlichkeit eines externen und eines internen DSB[6] erfordert die Berücksichtigung verschiedener Aspekte:

Generell hat ein externer DSB zwar eine längere Einarbeitungszeit, bis er genügend Einblick in die Organisation des Outsourcers bekommt. Dafür ist jedoch das Unabhängigkeitsgebot bei einem externen DSB eher gewährleistet als bei einem internen DSB, da der externe DSB nicht in die unternehmensinternen Netze „verstrickt" ist. Für die Entscheidung zu Gunsten eines externen DSB sprechen darüber hinaus Effektivität, Effizienz und die Haftung:

„Auch in der Haftungsfrage fährt der Arbeitgeber mit der Bestellung eines externen DSB meist günstiger, da dieser ihm gegenüber regelmäßig voll haftet und sich nicht auf die Grundsätze der betrieblich veranlassten Tätigkeit berufen kann."[7]

Durch die parallele Tätigkeit eines externen DSB bei verschiedenen Unternehmen können Synergieeffek-

te entstehen, welche die Vorteile des externen gegenüber dem internen DSB noch verstärken: So entfällt etwa das erstmalige Aufbauen des für die Tätigkeit des DSB erforderlichen Know-how. Darüber hinaus kann der externe DSB bei Bedarf auf Ressourcen in seinem Unternehmen zurückgreifen, z. B. indem er weitere unabhängige Personen, die über Spezialkenntnisse verfügen, oder Wissensdatenbanken heranzieht.

Generell kann der externe DSB seine Erfahrungen aus anderen Unternehmen nutzen, indem er standardisierte Vorgehensweisen entwickelt, die in Form von Arbeitsprogrammen umgesetzt werden. Hierbei entsteht ein economy of scale, den der Auftragnehmer an den Outsourcer weitergibt.

Die Bestellung eines externen DSB fördert außerdem ein konsequentes Vorantreiben des Datenschutzes innerhalb des Unternehmens. Der Auftraggeber möchte für seine Ausgaben eine entsprechende Gegenleistung. Der Auftragnehmer hingegen ist daran interessiert, möglichst umfassend für den Auftraggeber tätig zu werden.

Für einen internen DSB spricht insbesondere, dass dieser für Unternehmensangehörige und Dritte als ständiger Ansprechpartner zur Verfügung steht – zumindest wenn er hauptamtlich tätig ist. Zudem dürfte ein interner DSB bessere Kenntnisse über das Unternehmen besitzen und für den Datenschutz relevante Änderungen im Unternehmen früher erfahren als ein externer DSB.

Fazit

Ein externer DSB sollte immer dann engagiert werden, wenn es

- Interessenskollisionen zu vermeiden gibt – sei es auf Unternehmensebene oder auf Konzernebene,
- Datenschutz im Unternehmen mit hoher Priorität vorangetrieben werden soll,
- unternehmenseigene Resourcen nicht ausreichen und/oder
- nicht geplant ist, Ressourcen aufzubauen.

Nicht zuletzt sollte bei Unternehmen, die mit der Verarbeitung personenbezogener Daten im Rampenlicht der Öffentlichkeit stehen, auch die positive Außenwirkung eines extern bestellten Datenschutzbeauftragen genutzt werden.

Markus Bittner, Ernst & Young, Düsseldorf
Martin Derigs, Ernst & Young, Düsseldorf

Endnoten

1 Zur Begriffsbestimmung siehe § 3 BDSG.

2 Entwicklung des e-business von einfacher Informationsvermittlung bis hin zur Integration von Geschäftsprozessen siehe z. B. IFAC-Guideline E-Business and the Accountant: Risk Management für Accounting Systems in an E-Business Environment, in: Die Wirtschaftsprüfung, Heft 10/2002, S. 533–543, IDW-Verlag, Düsseldorf 2002.

3 Die Funktion eines Datenschutzbeauftragten gehört explizit zu der Gruppe der mit einer Tätigkeit als Wirtschaftsprüfer vereinbaren Tätigkeiten. Wirtschaftsprüfer-Handbuch, Institut der Wirtschaftsprüfer in Deutschland e.V., IDW-Verlag GmbH, Düsseldorf 2000, Rz. A 38. Vgl. auch WP Handbuch Band II, IDW-Verlag GmbH, Düsseldorf 1998, Rz. G 34.

4 Fachexamen des weltweiten Verbandes der IT-Revisoren, ISACA (Information Systems Audit and Control Association), Rolling Meadows, USA.

5 Vgl. Schlemann, Berndt: Recht des betrieblichen Datenschutzbeauftragten, Datakontext-Fachverlag, Köln 1996, S. 263.

6 Ebenda. S. 266 ff.

7 Ebenda. S. 269.

Datenschutz

Datenschutz im internationalen Unternehmensverbund

Einleitung

Die Thematik des Datenschutzes hat in den vergangenen Jahren für Unternehmen ebenso wie für deren Kunden und Mitarbeiter kontinuierlich an Bedeutung gewonnen. Veränderungen im unternehmerischen und technischen Umfeld werfen eine Vielzahl neuer datenschutzrechtlicher Fragen auf. Dies gilt insbesondere für die Sammlung und Verarbeitung personenbezogener Daten im internationalen Unternehmensverbund. Der vorliegende Beitrag nimmt diese Thematik auf und erläutert die rechtlichen, technischen und organisatorischen Hintergründe sowie Anforderungen an den internationaler Datentransfer innerhalb von Konzernen.

Aufbau internationaler und konzernübergreifender Datenverarbeitungsprozesse

In den vergangenen Jahrzehnten erlebten Unternehmen eine zunehmende Integration ihrer Geschäftsprozesse, die im Zeitalter multinationaler Konzerne und weit verflochtener internationaler Geschäftsaktivitäten vor Ländergrenzen keinen Halt machten. In der Regel getrieben durch Anforderungen an Effizienz und Effektivität erfolgte eine Integration der Prozesse internationaler Tochtergesellschaften von einer länderspezifischen Vernetzung bis hin zu einer globalen Zentralisierung einzelner unternehmerischer Aktivitäten.

Ermöglicht wurde diese Integration nicht zuletzt durch ein stetig steigendes Leistungsvermögen der betrieblichen Informationssysteme. Bedeutende Verbesserungen in Hardware und Software gingen einher mit der weitläufigen Vernetzung von Systemen, die sowohl auf leistungsfähigere Komponenten, als auch auf die weltweite Standardisierung der System-Kommunikation zurückzuführen ist. Enterprise Ressource Planning Software („ERP“), wie z. B. SAP R/3, BAAN oder Navision, begann ihren Siegeszug durch die Industrie.

Die Klassifizierung der in den Systemen verarbeiteten Daten macht deutlich, dass bei einer Vielzahl der integrierten Prozesse personenbezogene Daten betroffen sind, so z. B. bei den Prozessen der Personalabteilungen und des Marketings. Als unterstützende Technologie seien hier exemplarisch Personalsysteme („Human Ressource Planning“) sowie Customer-Relationship-Management („CRM“) Systeme angeführt. Oftmals sind diese Prozesse mit einem länderübergreifenden Datenfluss verbunden (vgl. Abbildung 1 für eine beispielhafte Personalabteilung).

Vielfach wird übersehen, dass international konsolidierte Systemarchitekturen aufgrund technischer Anforderungen oftmals auch für rein nationale Geschäftsprozesse einen internationalen Datenfluss notwendig machen (vgl. Abbildung 2). Das gilt zum Beispiel in dem Fall, in dem die Personalabteilungen verschiedener Konzernunternehmen ihre nationalen und auch internationalen Personalprozesse auf einem bei einem Konzernunternehmen zentralisierten Personalsystem abwickeln. Diese Komplexität in Prozessen und Technik ist für die meisten multinationalen Konzerne die betriebliche Realität.

Rechtliche Strukturierung der Konzern-Datenverarbeitung

Aus rechtlicher Sicht ist beim Aufbau solcher konzernweiten Datenverarbeitungssysteme entscheidend, dass die Datenübermittlungsvorschriften des Bundesdatenschutzgesetzes (BDSG) eingehalten werden. Die Weitergabe personenbezogener Daten bzw. die Gewährung von Zugriffsrechten an Mitarbeiter verbundener Unternehmen bedarf auch im Rahmen einer zentralisierten konzernweiten Datenverarbeitung grundsätzlich einer gesetzlichen Erlaubnis bzw. einer Einwilligung jedes einzelnen Betroffenen. Außerdem sind die im Zuge der Umsetzung der EG-Datenschutz-Richtlinie neu in das BDSG aufgenommenen Vorschriften zur Datenübermittlung ins Ausland zu beachten.

Insoweit gibt es für Datenweitergaben in einem Konzernverbund keine datenschutzrechtliche Privi-

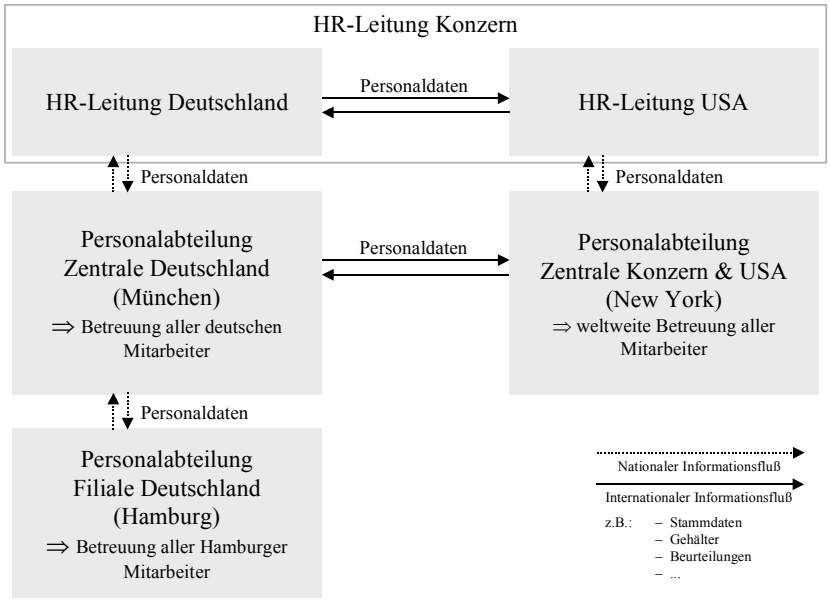


Abbildung 1: Schematische Darstellung einer internationalen Personalabteilung (Beispiel)

legierung. Das BDSG betrachtet die einzelnen konzernangehörigen Unternehmen untereinander als „Dritte“ gemäß § 3 Abs. 9 BDSG, behandelt den Unternehmensverbund also nicht als einheitliche „Verantwortliche Stelle“. Dasselbe gilt für den Austausch personenbezogener Daten zwischen rechtlich selbständigen Filialbetrieben. Lediglich eine Datenweitergabe zwischen unselbstständigen Zweigstellen, Zweigniederlassungen, Filialen, Betriebsstätten u. ä. untereinander bzw. mit der Hauptniederlassung stellt keine erlaubnispflichtige Übermittlung dar.

Kunden- und Mitarbeiterdaten dürfen also auch in einem Konzernverbund nicht frei zirkulieren. Auch wenn personenbezogene Daten also ausschließlich an andere Konzerngesellschaften übermittelt werden sollen, ist dies in einer etwaigen gesonderten Einwilligungserklärung des Betroffenen oder in der entsprechenden Klausel im Anstellungsvertrag besonders zu erwähnen. Auch im Rahmen einer solchen „Konzernklausel“ ist der Datenempfänger möglichst konkret mit Name (Firma) und Anschrift zu benennen.

Auftragsdatenverarbeitung

Die Einholung von Einwilligungserklärungen sämtlicher Kunden oder Mitarbeiter ist oftmals allerdings wenig praktikabel. Hier hilft die gesetzliche Privilegierung der sog. Auftragsdatenverarbeitung im Sinne von § 11 BDSG. Datenweitergaben im Rahmen einer Auftragsdatenverarbeitung sind nicht gesondert erlaubnispflichtig. Die Durchführung einer solchen Datenverarbeitung im Auftrag hat gemäß § 11 BDSG jedoch auf der Grundlage eines schriftlichen Vertrages zu erfolgen.

Eine Auftragsdatenverarbeitung liegt dann vor, wenn das datenverarbeitende Konzernunternehmen lediglich als weisungsgebundener (verlängerter) Arm oder als ausgelagerte Abteilung des Auftraggebers fungiert, der Auftraggeber also als „Herr der Daten“ die volle Verfügungsgewalt behält und Art, Umfang und Zwecke der Datenverarbeitung selbst bestimmt.

Die Datenübertragung zwischen dem Auftraggeber und dem Auftragnehmer stellt jedoch nur solange keine erlaubnispflichtige Datenübermittlung dar, wie der Auftragnehmer im Geltungsbereich der EG-Datenschutzrichtlinie ansässig ist. Wird die Auftragsdatenverarbeitung in einem Drittstaat vorgenommen, ist der Auftragnehmer gemäß § 3 Abs. 8 S. 3 BDSG als Dritter anzusehen, so dass die grenzüberschreitende Datenübertragung doch wieder als erlaubnispflichtige Übermittlung anzusehen ist. Davon unberührt bleibt freilich die grundsätzliche Zulässigkeit einer Auftragsdatenverarbeitung in einem Drittstaat. Für die Regelung solcher grenzüberschreitenden Auftragsverhältnisse hat die EG-Kommission kürzlich Standardvertragsklauseln entworfen, an denen sich die Konzernunternehmen orientieren sollten.

Funktionsübertragung

Die erwähnte Privilegierung gilt nur für eine echte Auftragsdatenverarbeitung, nicht aber für eine sog. Funktionsübertragung. Eine solche liegt vor, wenn einem Unternehmen neben der reinen Datenverarbeitung weitere, eigenständige Aufgaben übertragen werden, zu deren Erfüllung die Verarbeitung der Daten notwendig ist. Ein Fall der Funktionsübertragung liegt z. B. dann vor, wenn eine konzernangehörige Gesellschaft die gesamte Personaldaten-

verarbeitung einheitlich für alle Konzernfirmen betreibt und damit zumindest teilweise Aufgaben der Personalverwaltung mit übernimmt. Der Datenaustausch stellt dann eine Übermittlung im Sinne von § 3 Abs. 5 Nr. 3 BDSG dar, so dass in diesem Fall wiederum die Übermittlungsregeln des BDSG anwendbar wären. Die Abgrenzung, ob eine Outsorcing-Regelung als Auftragsdatenverarbeitung oder als Funktionsübertragung anzusehen ist, ist im Einzelfall vorzunehmen. Anzeichen für eine Funktionsübertragung ist insbesondere die Überlassung von Nutzungsrechten an den Daten.

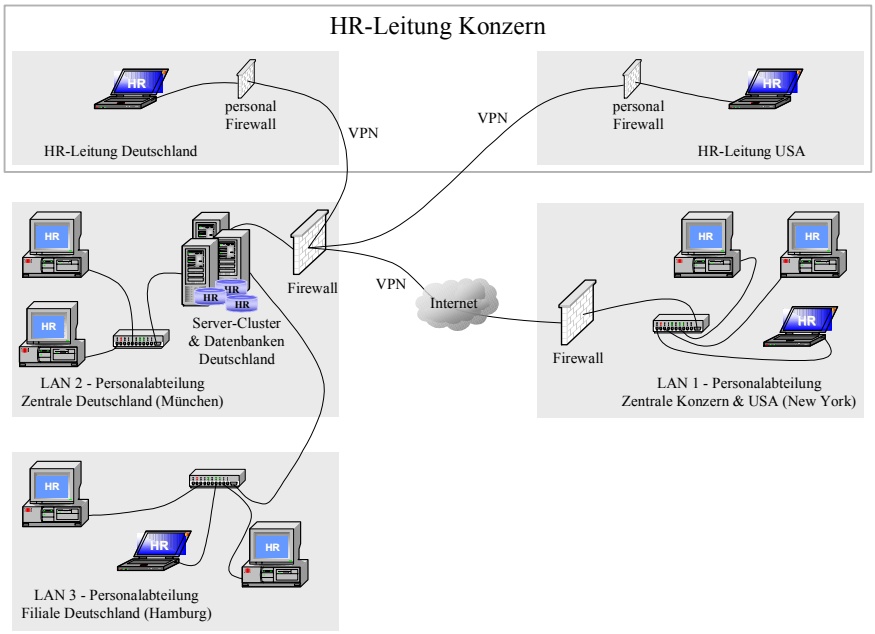


Abbildung 2: Schematische Darstellung des korrespondieren internationalen Personalsystems (Beispiel)

Gewährleistung eines angemessenen Datenschutzniveaus im Ausland

Ein gesondert zu betrachtender Problemkreis ist die Übermittlung personenbezogener Daten ins Ausland. Gemäß § 4 b und c BDSG gelten für die Übermittlung personenbezogener Daten an Stellen außerhalb des Europäischen Wirtschaftsraumes (EWR) – unbeschadet der dargestellten Anforderungen – weitere spezifische Zulässigkeitsvoraussetzungen.

Grundsätzlich gilt, dass Daten nicht an Stellen außerhalb des EWR übermittelt werden dürfen, wenn dort ein „angemessenes Schutzniveau“ nicht gewährleistet ist. Sollten Mitarbeiter von verbundenen Unternehmen, die ihren Sitz außerhalb des EWR haben, Zugriff auf personenbezogene Daten von Mitarbeitern einer deutschen Gesellschaft oder Niederlassung erhalten, läge hierin eine Übermittlung in einen Drittstaat, die ein angemessenes Datenschutzniveau im Empfängerland voraussetzt.

In Anbetracht der Tatsache, dass weltweit bislang nur ca. 35 Staaten über Datenschutzgesetze verfügen, und davon nicht alle dem EG-Schutzstandard entsprechen, ist davon auszugehen, dass nur wenige Drittstaaten die Anforderungen an ein angemessenes Schutzniveau erfüllen. Die Zulässigkeit eines Datenexports in diese Länder hängt dann regelmäßig davon ab, ob die Aufsichtsbehörden Ausnahmen im Einzelfall zulassen.

Die EG-Kommission hat bisher die Angemessenheit des Schutzniveaus der Datenschutzregimes der Schweiz, Ungarns, Kanadas und der USA – letzteres nach Maßgabe der sog. „Safe Harbour-Grundsätze“ – festgestellt. Ein Datenexport in diese Länder ist dadurch erheblich erleichtert worden. Die Entscheidungen der Kommission sind für alle Mitgliedstaaten bindend, so dass Datenübermittlungen in diese Länder durch die mitgliedstaatlichen Aufsichtsbehörden nicht mehr wegen eines unzureichenden Datenschutzniveaus unterbunden werden können. Dies gibt den grenzüberschreitend tätigen Konzernen die notwendige Rechtssicherheit.

Die BDSG-Novelle berücksichtigt die Anforderungen internationaler Konzerne zudem im Rahmen von § 4 c Abs. 2 S. 1 BDSG. Danach kann die zuständige Aufsichtsbehörde einen Datenexport in Drittstaaten, die kein hinreichendes Datenschutzniveau im Sinne von § 4 b Abs. 3 BDSG gewährleisten, ausnahmsweise dann genehmigen, wenn sich ausreichende Datenschutzgarantien aus verbindlichen Unternehmensregelungen ergeben. Dadurch wird es den Konzernen ermöglicht, einen ausreichenden Datenschutzstandard dadurch herzustellen, dass für alle Teilunternehmen unabhängig von

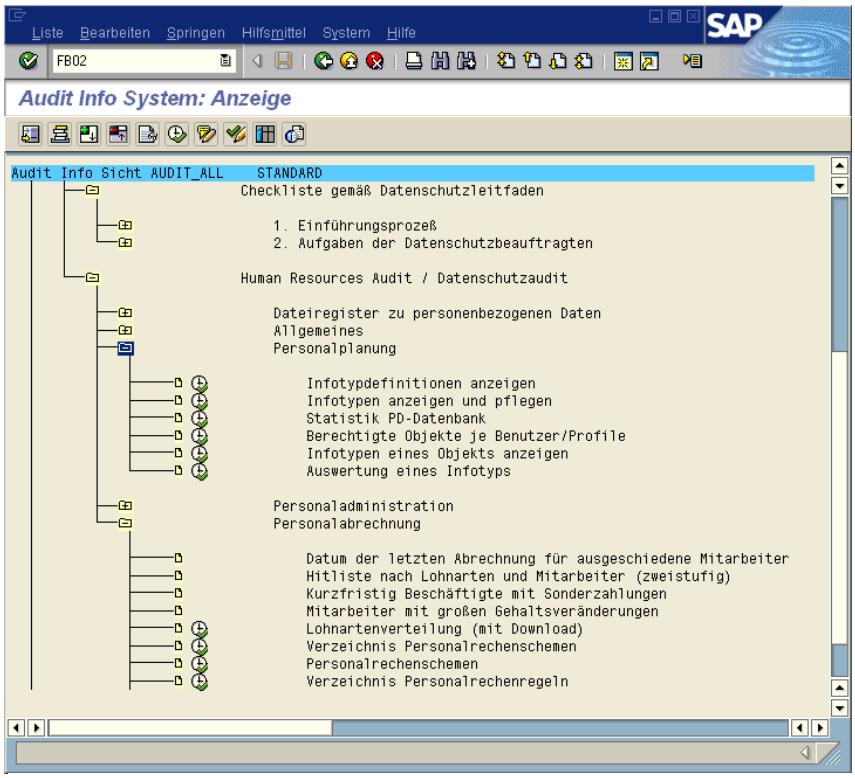


Abbildung 3: Auszug datenschutzrechtlicher Aspekte Audit Info System SAP R/3

ihrem Standort verbindliche Regelungen über den Datenschutz („codes of conduct“) etabliert werden. Um beim Export von Daten in Drittstaaten ohne angemessenes Schutzniveau in den Genuss dieses Privilegs zu kommen, müssen diese codes of conduct jedoch zuvor der zuständigen Aufsichtsbehörde zur Genehmigung vorgelegt werden. Für Konzernmütter und ihre Töchter bedeutet dies, dass Genehmigungen von allen rechtlich selbständigen Unternehmen für ihre Datenübermittlungen bei der jeweils zuständigen Aufsichtsbehörde zu beantragen sind. Bei Konzerndatenverarbeitungen besteht deshalb oft eine Genehmigungszuständigkeit mehrerer Aufsichtsbehörden. Um das Genehmigungsverfahren zu beschleunigen, sollte bei der Behörde am Sitz der Konzernmutter oder bei derjenigen Behörde, bei der der erste Genehmigungsantrag gestellt wird, deshalb darauf hingewirkt werden, intern die Federführung für alle Genehmigungsverfahren zu übernehmen.

Ausgewählte rechtliche, technische und organisatorische Maßnahmen

Für eine rechtskonforme Systemgestaltung ist es für jeden internationalen Konzernverbund unumgänglich, zunächst die Komplexität an Prozessen, Technologien und bestehenden Datenschutzmaßnahmen zu durchdringen und sämtliche personenbezogenen Datenströme zumindest auf aggregierter Basis zu ermitteln. Ob bei dieser Bestandesaufnahme zentral oder dezentral vorgegangen und technische Hilfsmittel eingesetzt werden, ist abhängig von den unternehmensspezifischen Gegebenheiten. Wesentlich für die Aufnahme der Daten ist die parallele Betrachtung der Verarbeitung im Sinne von Geschäftsprozessen und eingesetzter Technologie, da hier deutliche Abweichungen zu erwarten sind. Eine zentralisierte und portalgestützte Erfassung und Klassifizierung der Datenströme und der damit verknüpften Informationen zu Prozessen, Technik und Datenschutzmaßnahmen ist eine der vielen Möglichkeiten, eine angemessene Ausgangsbasis für die Beurteilung datenschutzrechtlicher Fragestellungen zu gewinnen. Neben eigenständigen technischen Hilfsmitteln können auch bereits bestehende Informationsmöglichkeiten genutzt werden. SAP stellt z. B. hierzu in R/3 das Audit Info System („AIS“) zur Verfügung, welches ab Release 4.6. im R/3-Standard enthalten ist (vgl. Abbildung 3).

Im Anschluss an die Bestandesaufnahme können weitere rechtliche, technische und organisatorische Maßnahmen definiert und priorisiert werden.

Grundsätzlich gilt, dass die in § 9 BDSG und der dazugehörigen Anlage geforderten technischen und organisatorischen Maßnahmen zu gewährleisten sind. Die durchzuführenden technischen Maßnahmen werden sich, vereinfacht formuliert, im wesentlichen auf die Sicherstellung des physischen und logischen Zugriffschutzes konzentrieren. Bei dem in Abbildung 2 dargestellten technischen Umfeld würde der Schwerpunkt auf dem Zugriffschutz des zentralen Personalsystems und der verbindenden Netzwerke (intern und extern), liegen. Organisatorische Maßnahmen müssen in diesem Zusammenhang ebenfalls berücksich-

tigt werden (z. B. Vergabe der Zugriffsrechte, Network Intrusion Detection etc.).

Eine vielmals untergeordnete Rolle, wenngleich in der Bedeutung von nicht zu unterschätzender Relevanz, hat die Analyse technischer Verarbeitungsverfahren. Die von Anwendern wahrgenommene Speicherung, Übermittlung bzw. Verarbeitung von personenbezogenen Daten kann in ihrem technischen Umfang weitaus umfassender ausfallen und sollte daher von betrieblichen Datenschutzbeauftragten proaktiv hinterfragt werden. Werden zum Beispiel übermittelte Daten tatsächlich auf definierte Felder beschränkt, oder liefert das System intern vollständige Datensätze? Werden mehr Kundendaten erhoben und gespeichert als zunächst ausgewertet? Fragestellungen die, sofern bejaht, geltendem Datenschutzrecht widersprechen können.

Aus datenschutzrechtlicher Perspektive wäre insoweit sicherzustellen, dass die Datenerhebungen, -verarbeitungen und -übermittlungen auf das zulässige Maß beschränkt, bzw. die zugrundeliegenden vertraglichen Regelungen den datenschutzrechtlichen Erfordernissen angepasst und etwaig erforderliche Genehmigungen der Aufsichtsbehörden eingeholt werden. Bei Datentransfers ins Nicht-EWR-Ausland sollten zwischen den datenimportierenden und den datenexportierenden Konzernunternehmen zumindest Datenschutzvereinbarungen nach Maßgabe der Standardvertragsklauseln der EG-Kommisssion abgeschlossen werden. Im Rahmen eines ganzheitlichen Ansatzes würde es sich außerdem anbieten, die im BDSG vorgesehenen Selbstregulierungsmechanismen auszunutzen und konzernweite Unternehmensregelungen auf dem Gebiet des Datenschutzes und der Datensicherheit („codes of conduct“) z. B. in der Form einer Betriebsvereinbarung zu etablieren.
Daneben existieren weiterführende Anforderungen organisatorischer Natur, die innerhalb des Konzernverbundes sichergestellt werden müssen. Eine der wesentlichsten und zugleich anspruchvollsten Maßnahmen stellt die Einführung und Sicherstellung von Change Management-Prozessen dar, die Veränderungen in Datenströmen und datenschutzrechtlichen Maßnahmen erkennen und zielführend adressieren müssen. Die kontinuierliche datenschutzrechtliche Ausbildung aller Mitarbeiter, die mit personenbezogenen Daten arbeiten, ist eine weitere bedeutende Herausforderung. Internationale Unternehmen werden auch hier vielfach den Einsatz von zentralen und toolgestützten Verfahren bevorzugen, wie z. B. die Absolvierung von Computer Based Trainings („CBT“) per Web-Portal. Gleichfalls empfehlenswert ist die Durchführung interner Datenschutzprüfungen, da diese als interner Kontrollmechanismus die Effizienz und Effektivität der Datenschutzmaßnahmen verbessern können. Derartige Prüfungen können sowohl mit anderen internen Prüfungen (z. B. der internen Revision) kombiniert, als auch gesondert vollzogen werden.

Fazit

Neben der Verantwortung gegenüber Mitarbeitern und Kunden wird auch die in diesem Umfeld erhöhte Aufmerksamkeit der Aufsichtbehörden dazu beitragen, dass der Datenschutz im internationalen Unternehmensverbund in Zukunft an Bedeutung gewinnen wird. Diese für zahlreiche Konzerne herausfordernde Aufgabe gilt es im Zusammenspiel von Recht, Technik und Organisation zu meistern. Allerdings werden nur gut ausgebildete multidisziplinäre Teams die verflochtenen Problemstellungen angemessen identifizieren und lösen können.

Michael Isensee,
TSRS Ernst & Young AG WPg,
Hamburg

Dr. Flemming Moos,
Luther Menold
Rechtsanwaltsgesellschaft mbH –
Ernst & Young Law Alliance,
Hamburg

Datenschutz

La protection des données : pourquoi et comment ?

De tous les besoins de sécurite traditionnels (Disponibilité – avoir l'information au bon moment –, Intégrité – avoir l'information juste –, Confidentialité – avoir l'information pour la bonne personne), la confidentialité et l'intégrité sont les facteurs les plus représentatifs de la sécurité des systèmes d'informations. Ce besoin est en effet demandé pour des types de données communes à chaque entreprise (informations comptables, données commerciales, stratégie d'entreprise, secrets de fabrique, etc.).

On l'oublie souvent, mais le besoin de protection des données peut être exigé par des contraintes réglementaires ou légales. Ainsi, en ce qui concerne les données nominatives, depuis la création de la Commission Nationale de l'Informatique et des Libertés (CNIL) en 1978, on prend de plus en plus conscience de la préservation des libertés individuelles. Toute entreprise désireuse de constituer un fichier de données nominatives est sujette à certaines obligations et à certains devoirs. Un peu plus tard, le législateur français a souhaité créer une loi protégeant les données (et les traitements), définissant ainsi la notion de « criminalité informatique ». Pour remplir ces obligations légales ou réglementaires, les entreprises disposent de plusieurs mécanismes de sécurité logique.

Une loi qui réglemente les données

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a pour objectif de protéger les droits et libertés des personnes individuelles au regard de la création et de l'exploitation de traitements automatisés d'informations nominatives. On considère une information comme « nominative » si elle permet l'identification d'une personne physique de manière directe (par exemple le nom) ou indirecte (comme le numéro de sécurité sociale).

La collecte des informations nominatives est donc réglementée par des interdictions et des conditions. Il est en effet interdit de collecter des informations sur l'origine raciale, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou mœurs des personnes ainsi que des informations relatives à la santé. Il existe néanmoins certaines dérogations applicables uniquement dans des cas très stricts (pour la presse par exemple, ou pour les médecins lorsqu'ils sont liés par le secret professionnel). Par ailleurs, la collecte des informations est soumise à des conditions : les personnes auprès desquelles sont recueillies les informations doivent être informées du caractère obligatoire ou facultatif des réponses, doivent disposer d'un droit d'accès et de modification. De plus, une collecte qui aurait été opérée par un moyen frauduleux, déloyal ou illicite est interdite.

Ce qui est souvent négligé lors de la mise en place d'un traitement de données nominatives, c'est l'aspect réglementaire de la conservation de ces informations. En effet, il est précisé dans la loi que « Toute personne ordonnant ou effectuant un traitement s'engage vis-à-vis des personnes concernées à prendre toutes précautions utiles afin de préserver la sécurité des informations et d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ». Le non respect de cette obligation de résultat peut entraîner de lourdes sanctions prévues par l'article 226-17 du nouveau code pénal : « le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de 5 ans d'emprisonnement et de 2 000 000 F d'amende ».

Une loi qui protège les données

En janvier 1988, le législateur a créé un arsenal juridique permettant de poursuivre les auteurs coupables d'infractions liées à des systèmes informatiques selon differentes notions.

L'accès (ou le maintien) frauduleux dans un systeme informatique : définit l'acte d'accéder à des données ou à un traitement contre la volonté du

« maître du système ». Ce concept va bien au-delà du simple « vol d'information » (que le dispositif juridique ne prévoit pas) mais bien de l'accès (pour « voler », il faut préalablement avoir eu accès), ainsi la simple consultation non autorisée est considérée comme frauduleuse. A noter que l'infraction peut être constituée même si le système attaqué n'est pas pourvu de protection particulière. En effet, cette obligation de protection n'a pas été définie car elle aurait été générique, donc imprécise dans la loi, ou alors trop technique, donc précise dans la loi en risquant de devenir obsolète avec les évolutions technologiques. Notons enfin que, pour que cette disposition de la loi puisse être applicable, il faut prouver que l'accès a bien été réalisé contre la volonté du maître du système et donc indiquer clairement dans le système (au moment de la connexion d'un utilisateur par « identifiant/mot de passe » par exemple) quelles sont les catégories de personnes autorisées à accéder au système et quelles sont les catégories qui ne le sont pas.

La notion d'atteinte au système ou aux données est beaucoup plus liée aux besoins de sécurité que sont l'intégrité et la disponibilité. En effet, « l'atteinte » se caractérise par l'altération ou l'entrave au fonctionnement du système (performances dégradées, erreurs de calculs…), la suppression ou la modification de données ainsi que tout dommage induit par l'action d'un piratage ou l'introduction de virus.

Le tableau dresse une synthèse de quelques infractions (liste non exhaustive) liées aux deux lois mentionnées.

Infraction	Amende	Prison
Réaliser un traitement nominatif sans respecter les formalités préalables	300 000 F.	3 ans
Ne pas sécuriser les données nominatives	2 000 000 F.	5 ans
Traitement comprenant des données non autorisées	2 000 000 F.	5 ans
Détournement de finalité d'un traitement de données nominatives	2 000 000 F.	5 ans
Accès frauduleux à un système informatique	100 000 F.	1 an
Altération, modification des données d'un système informatique	200 000 F.	2 ans

Les méchanismes de protection des données : la sécurité logique

On considère un mécanisme de « sécurité logique » tout mécanisme de sécurité permettant de réduire le risque d'atteinte à l'information de manière non physique (une atteinte « physique » est provoquée par exemple par bris d'ordinateur, dégât des eaux, incendie, vol de machine, etc.).

L'authentification

L'authentification est une fonction de sécurité permettant d'avoir la certitude que la personne est bien celle qu'elle prétend être. Le mécanisme d'authentification le plus connu est le couple « identifiant/mot de passe ». Lorsque l'on saisit son identifiant (nom d'utilisateur), on décline son identité ; lorsqu'on saisit le mot de passe on prouve son identité par la connaissance d'un secret associé à l'identité.

Il existe plusieurs techniques d'authentification:

- Authentification par ce que l'on sait : typiquement un mot de passe, un code,
- Authentification par ce que l'on a : par exemple un badge, une carte à puce,
- Authentification par ce que l'on est : il s'agit alors des mécanismes d'authentification biométrique liée et unique à chaque personne (empreinte d'un doigt, reconnaissance vocale, identification retinienne…)

Naturellement, il est possible de combiner ces trois techniques élevant ainsi le niveau de sécurité (par exemple en enregistrant sur une carte à puce l'empreinte d'un doigt de l'utilisateur et en associant un code secret pour y accéder).

Le contrôle d'accès

Les techniques de contrôle d'accès logique permettent de définir quels sont les utilisateurs qui peuvent accéder à telle ou telle ressource du système informatique. Par exemple, définir de manière logicielle qu'un groupe de personnes peut réaliser des impressions sur une imprimante particulière, alors que les autres utilisa-

teurs n'appartenant pas à ce groupe ne peuvent pas le faire.

Les mécanismes de contrôle d'accès logique s'appliquent également (et surtout) sur des données : elles peuvent être accessibles avec plusieurs fonctionnalités distinctes (droit de lecture, droit d'écriture, droit d'exécution s'il s'agit d'un programme) définies dans ce qu'on appelle des « listes de contrôle d'accès » (Access Control List).

La journalisation

La journalisation permet d'assurer une fonction de sécurité peu connue des « sécuriticiens » mais pourtant indispensable pour des auditeurs financiers, par exemple, puisqu'il s'agit de l'Auditabilité (faculté de prouver l'information et les processus qui ont permis de l'établir).

En effet, les techniques de journalisation, permettent de définir des pistes d'audit indiquant par exemple quel utilisateur (ou programme) a réalisé la dernière manipulation sur une donnée, quel utilisateur a demandé une impression de tel fichier.

En étudiant les journaux (log) produits par les différents systèmes, il est possible, par exemple, de réaliser des enquêtes comportementales sur les habitudes de connexion et de détecter un problème potentiel. En effet, si on détecte qu'un utilisateur donné a pour habitude de se connecter au réseau d'entreprise de 8 h 30 à 19 h et que soudainement il lui arrive de rester connecté jusqu'à minuit, on peut déduire quelques hypothèses : il a une charge de travail importante en ce moment, il est en retard sur ses projets… ou bien il peut réaliser des opérations contraires aux intérêts de l'Entreprise. On voit donc que ces journaux peuvent être particulièrement sensibles, et il s'agira avant tout de les sécuriser au maximum et de ne les exploiter qu'à bon escient.

Le chiffrement

On connaît le chiffrement (plus communément appelé, à tort, « cryptage » – mot qui n'existe pas dans la langue française) dans la vie courante comme un mécanisme permettant, par exemple, de brouiller les émissions d'une chaîne de télévision à péage. On parle aussi de plus en plus de la nécessité de chiffrer ses informations bancaires (numéro de carte de crédit) lors de transactions de commerce électronique sur Internet.

Le chiffrement est en effet un mécanisme qui permet de rendre illisible des données pour des personnes qui ne posséderaient pas la clé de déchiffrement (opération inverse du chiffrement). Le décryptage consiste à essayer de retrouver les données originales, sans avoir la clé de déchiffrement.

Il existe plusieurs méthodes de chiffrement (algorithmes) dont la robustesse (capacité à résister au décryptage) dépend à la fois de leur conception mathématique, mais aussi de leurs longueurs de clés mesurées en bits. En effet, il est beaucoup plus difficile de décrypter un message chiffré à l'aide d'un algorithme « triple DES » (168 bits), qu'à l'aide d'un DES simple (56 bits). Parmi les algorithmes de chiffrement on distingue les algorithmes à clés symétriques (la clé qui permet de chiffrer est la même qui permet de déchiffrer) et les algorithmes à clés asymétriques (la clé qui permet de chiffrer est différente de celle qui permet de déchiffrer). Les algorithmes à clés symétriques ont la propriété d'être rapides en termes de temps de calcul, mais soulèvent le problème du partage des clés; alors que les algorithmes à clés asymétriques demandent beaucoup plus de temps de calcul, mais la gestion des clés est plus simplifiée.

Concrètement et à titre d'exemple, le chiffrement actuellement utilisé en France sur Internet pour les transactions sécurisées de commerce électronique est de type « asymétrique » (avec une première phase de « négociation » symétrique) avec une longueur de clés de 40 bits.

Notons enfin qu'à ce jour l'utilisation du « chiffrement fort » (longueur de clés équivalente à plus de 128 bits) est soumise à réglementation en France.

Le scellement

Le scellement de données permet de garantir leur intégrité, c'est-à-dire avoir la certitude qu'elles n'ont pas été modifiées ou altérées. On peut assimiler le scellement de données à des informations qu'on aurait mises dans une enveloppe fermée et cachetée avec un sceau en cire.

D'un point de vue technique, on utilise des méthodes de « condensa-

tion » : par exemple d'un fichier de 1000 caractères, on génèrera avec une formule mathématique un condensat de 50 caractères (appelons-le « C »). De ce condensat on ne peut pas retrouver le fichier original, mais pour chaque fichier original on ne peut réaliser qu'un seul condensat. Ainsi si le fichier original est modifié, le condensat généré « C' » sera forcément différent de « C », d'où la preuve qu'il y a eu altération.

La non-répudiation

La non-répudiation est la preuve qu'une action a bien été réalisée, comme lorsqu'on signe l'accusé de réception d'une lettre recommandée : on ne peut nier avoir reçu la lettre.

La non-répudiation fait souvent intervenir la notion de signature électronique (qui vient d'être reconnue légale par le parlement français, au même titre que la signature scripturale). En effet, une personne qui envoie un fichier et signe ce fichier ne peut nier avoir envoyé ce fichier ; de la même manière une personne qui reçoit un fichier peut générer un accusé de réception et le signer : elle ne pourra pas nier l'avoir reçu.

On l'a vu, la diversité des mécanismes de sécurité logique permet de répondre à de nombreux besoins de sécurité de l'information. Mais rappelons, comme toujours, qu'il ne suffit pas de disposer de tels mécanismes : encore faut-il savoir les mettre correctement en œuvre, de les faire appliquer par les différents utilisateurs, de disposer de moyens de contrôle afin de ne pas avoir une fausse vision de sa propre sécurité.

Frédéric Huynh, Auditeur-conseil
Secrétaire Général du CLUSIF

Nachdruck mit der Bewilligung der AFAI

CISM

Braucht unsere Gesellschaft den neuen Titel?

In den ISACA-News vom November 2002 kündigt Robert Roussey im Namen des Board of Directors der ISACA stolz den Certified Information Security Manager (CISM) an. Der Inhaber dieses einzigartigen Titels soll sich mit der Handhabung (*management*) der Informationssicherheit, weniger mit einzelnen Systemen oder allgemeinem Sicherheitswissen auseinandersetzen.

Aber tut dies nicht bereits der CISA? Eine in letzter Zeit im Zusammenhang mit dem neuen Titel wohl oft gestellte Frage. Tut er. Aber nicht ausschliesslich und nicht fokussiert. Der CISA ist definitionsgemäss Revisor der Informationstechnologie. Gerade aufgrund von COBIT und den darin enthaltenen Beschreibungen beschäftigt er sich auch mit der Kontrolle (*control*) und der Beherrschung (*governance*) dieser Materie. Um die Informationstechnologie kontrollieren und beherrschen zu können, gehören die Aspekte der Sicherheit an prominenter Stelle mit zu diesen Aufgaben. Darf der CISA demnach für sich in Anspruch nehmen, die Voraussetzungen für diesen neuen Titel zu erfüllen?

Ja und nein. Meiner Meinung nach ja, weil er den Inhalt der notwendigen Sicherheitsmassnahmen im Umfeld der Informationstechnologie kennen muss. Er sollte damit sogar vertraut sein. Nein, weil er sich mit den vielen andersartigen Aufgaben nicht ausschliesslich auf die Aspekte der Informationssicherheit konzentrieren kann. Aber rechtfertigt diese Aussage eine neue Prüfung mit einem neuen Titel?

Einer meiner ersten Lehrmeister im Revisionsberuf meinte einmal in einem Anfall von Selbsterkenntnis: „Ich betrachte mich als guten Analysten. Wenn ich ein Macher wäre, würde ich mich als Unternehmer betätigen, und nicht als Revisor.“ Treffer.

Des öftern werden die guten Ratschläge der Revisoren belächelt. Oder in den Wind geschlagen. Als nicht kosteneffizient beurteilt oder als abstrakt-theoretisch verworfen. Nur, wenn etwas schief läuft, ist dann schnell der Rechtsanwalt mit einer Haftungsklage zur Hand.

Ich habe mich schon immer ein bisschen daran gestossen, dass die Revisoren im allgemeinen und die Informatikrevisoren im speziellen für sich in Anspruch nahmen, bezüglich Wirksamkeit, Leistungsfähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Gesetzestreue und Zuverlässigkeit (merken Sie COBIT?!) alles besser wissen wollen, ohne sich unter Umständen je auf Seiten der Ausführung bezüglich dieser Ordnungsmässigkeitsstichworte betätigt zu haben. Der neue Titel, so verstehe ich es wenigstens, will sich auf die direkte *Bearbeitung* der Problemkreise der Informationssicherheit (*management*) konzentrieren. Mancher bereits heute als Sicherheitsbeauftragter oder -manager eingesetzte (missbrauchte?) Informatikrevisor bzw. CISA wird die neue Berufsbezeichnung begrüssen. Er wird sich in seiner Rolle als Zahnrad im Regelkreis der Unternehmung mit dem neuen Titel besser zurechtfinden, weil dieser seinen Verantwortungsbereich genauer umschreibt. Wo er bisher vielleicht seine Tätigkeit als etwas unter seiner „Würde“ als CISA betrachtete, sieht er diese anerkannt und zumindest als gleichwertig eingestuft.

In diesem Sinne bin ich überzeugt, dass sowohl der neue Titel CISM als auch der bestehende des CISA gewinnen werden: Der CISM sieht den Umgang mit der Informationssicherheit im Brennpunkt des Interesses, der CISA konzentriert sich auf seine ursprüngliche Bestimmung, die Revision.

Die Koordinaten für die Beschreibung des Berufsbildes und der Möglichkeit, den CISM zu erwerben sind:
www.isaca.org/cismcont1.htm (Information Security Governance),
www.isaca.org/cismcont2.htm (Risk Management),
www.isaca.org/cismcont3.htm (Information Security Program Management),
www.isaca.org/cismcont4.htm (Information Security Management) und
www.isaca.org/cismcont5.htm (Response Management).

Ich freue mich darauf, die ersten CISM im schweizerischen bzw.

deutschsprachigen Raum an einer nächsten ISACA-Veranstaltung begrüssen zu dürfen.

Max F. Bretscher, Langnau a/A

CISM

Le CISM, une combinaison gagnante

Le CISM, une combinaison gagnante

L'ISACA vient de crér une nouvelle certification nommé CISM (Certified Information Security Manager) destiné aux managers expérimentes en Sécurité des Systèmes d'information et à ceux qui disposent de responsabilités dans le domaine de la sécurité. Le CISM est conçu pour apporter aux dirigeants une garantie que les collaborateurs certifiés disposent des connaissances répondant aux standards de performance internationaux et des compétences nécessaires au management et au conseil en Sécurité. Ce diplôme orienté métier et gestion des risques informatiques aborde les problématiques de Sécurité en terme de management, de conception et de mise en œuvre.

Comment obtenir le CISM ?

Deux possibilités sont offertes aux candidats pour obtenir le CISM.

La première consiste à passer et réussir l'examen du CISM. Le premier examen du CISM aura lieu courant juin 2003 dans les mêmes centres d'examen que le CISA, à savoir dans environ 200 sites répartis dans prés de 75 pays. Pour la France, il s'agira du centre de Paris. Pour les candidats ayant passé avec succès l'examen écrit, la validation de la certification n'est obtenue qu'après :

- Adhésion au code d'éthique professionnel de l'ISACA et acceptation d'un suivi de formation professionnelle continue sur le domaine.
- Justification d'un minimum de cinq années d'expérience professionnelle dans le domaine de sécurité des systèmes d'information dont trois années minimum dans le rôle de manager en sécurité des systèmes d'information.

Des équivalences existent et peuvent être comptabilisées en année d'expérience professionnelle. Ainsi, par exemple un auditeur CISA, un professionnel certifié CISSP ou un détenteur d'un diplôme de troisième cycle en sécurité des systèmes d'information peut obtenir une équivalence de deux années d'expérience. Une expérience en management de système d'information ou une certification GIAC, MCSE, CBCP ou CompTIA Security plus équivaut à une année d'expérience. Un cumul n'est en revanche pas possible. De plus, une expérience de trois ans comme manager en sécurité des systèmes d'information est un prérequis indispensable.

La seconde offerte jusqu'au 31 décembre 2003 : les personnes possédant huit années ou plus d'expérience, dont cinq minimum dans le rôle de manager en sécurité des systèmes d'information, peuvent également demander I'obtention de la certification CISM sans avoir à passer l'examen. D'autres équivalences peuvent également être obtenues. Pour plus d'informations sur ce processus de « Grandfathering », vous pouvez contacter directement l'AFAI.

Quels sont les domaines abordés par le CISM ?

Pour concevoir le CISM, l'ISACA a consacré plus de deux ans à collecter des informations pointues sur la sécurité des systèmes d'information et à les faire valider par des tiers de référence sur le sujet. Le fruit de ces travaux a permis notamment d'identifier les connaissances indispensables exigées pour faire d'un collaborateur en sécurité un véritable manager en sécurité des systèmes d'information.

Le CISM couvre ainsi un certain nombre de domaines comprenant :

- Gouvernance de la sécurité : s'assurer que la stratégie en terme de

sécurité des systèmes d'information est en ligne avec les objectifs business de l'entreprise et en accord avec les contraintes juridiques et réglementaires. Les thèmes abordés comprennent notamment la politique sécurité, l'organisation sécurité, la définition des rôles et responsabilités.

- Risk Management : identifier et gérer les risques relatifs à la séurité des systèmes d'information afin d'atteindre les objectifs business. Les thèmes abordés comprennent notamment le développement d'un processus d'analyse des risques, les méthodologies d'analyse de risques, le choix des stratégies et l'élaboration de plan d'actions permettant de gérer ces risques.
- Schéma directeur de la sécurité des systèmes d'information : concevoir, développer et manager une stratégie pour mettre en œuvre les principes établis par la gouvernance de la sécurité. Les thèmes abordés comprennent notamment la conduite de projet, le cycle de développement, l'architecture de sécurité.
- Gestion de la sécurité : mettre en œuvre les orientations contenues dans le schéma directeur de la sécurité. Les thèmes abordés comprennent notamment les tableaux de bord, le budget sécurité, l'audit et contrôle, la formation.
- Gestion de crise : être en mesure de répondre efficacement et de redémarrer face à des incidents de la sécurité des systèmes d'information. Les thèmes abordés comprennent notamment la gestion d'incident, le plan de secours, le plan de continuité d'activités.

Les atouts de la certification CISM

Les personnes ayant passées le CISA ces dernières années auront constaté une évolution de plus en plus importante du domaine concernant la Sécurité. En effet, la sécurité des systèmes d'information prend aujourd'hui une place stratégique au sein de I'entreprise. Pour cette raison notamment, L'ISACA a créé le CISM dédié au management de la sécurité des systèmes d'information.

Contrairement aux autres certifications disponibles aujourd'hui et portant soit sur des plate-formes spécifiques soit sur des problématiques générales ou techniques, le CISM repose sur le développement de nouvelles compétences, liées au management de la sécurité, chez les professionnels expérimentés en sécurité de l'information. De plus, les certifies adhèrent à une communaute d'intérêt mutuel, véritable lieu d'échanges et de dialogues.

L'obtention du CISM apporte une preuve tangible d'une véritable progression de carrière : en effet, la réussite à l'examen base sur l'expérience du terrain indique une expérience solide couplée d'une véritable expertise en management de la sécurité informatique. Le CISM peut constituer une méthode à la disposition de la direction générale d'évaluation des équipes spécialisés en place mais aussi servir de critères de choix dans les processus de recrutement. Le CISM est délivré par l'ISACA qui propose déjà depuis de nombreuses années à la fois une certification en audit des systèmes d'information (CISA) reconnue au niveau international comme étant un symbole d'excellence dans la profession de l'audit informatique.

L'AFAI, en partenariat avec le CLUSIF et le CIGREF, se charge de la mise en place du CISM en France. Aussi, elle se tient à votre disposition pour toute question complémentaire concernant le CISM et les modalités d'inscription.

Dominique Van Egroo/
François Daure

Nachdruck mit der Bewilligung der AFAI.

Express Line

A Word from the Chair

It is hard to believe that 2003 is upon us. For all chapters, this year is going to be an exciting and challenging one. To make progress, we will need to surpass last year's achievements while addressing the ever-changing needs of our constituency. Best wishes for a happy, healthy new year!

CISM Exam Coverage

The CISM Certification Board recently approved the allocation of questions by area for the CISM exam (see areas and percentages in the following list). These percentages were derived from the job practice analysis recently conducted with industry practitioners.

- Information security governance – Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. (21%)
- Risk management – Identify and manage information security risks to achieve business objectives. (21%)
- Information security program(me) management – Design, develop and manage an information security program to implement the information security governance framework. (21%)
- Information security management – Oversee and direct information security activities to execute the information security program. (24%)
- Response management – Develop and manage a capability to respond to and recover from disruptive and destructive information security events. (13%)

CISM Study Materials

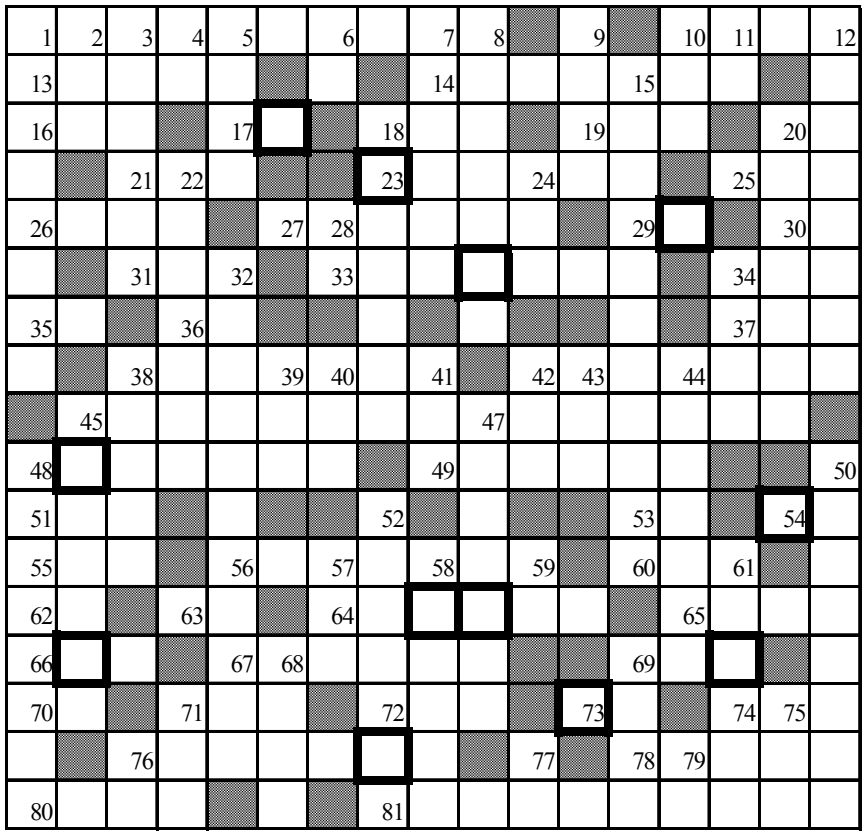
The *CISM Review Manual* will be available in February 2003 to assist individuals in preparing for the CISM exam. The manual will feature detailed descriptions and explanations of task and knowledge statements and provide applicable information security management principles, practices and strategies with references to where additional guidance can be found. A CISM study course PowerPoint presentation also is being developed to follow the study guide and will be available to ISACA chapters in February 2003. contact Terry Trsar at *ttrsar@isaca.org*.

GRA Board Gets Underway

One of ISACA's newest key boards has begun operations. The Governmental and Regulatory Agencies (GRA) Board exists to ensure that ISACA's initiatives with multinational bodies are coherent and consistent, making effective use of the association's resources and global perspective for the benefits of members. The GRA Board will focus on multinational issues and opportunities within a geographic area, or opportunities that can be defined as providing exposure or benefits to a wider constituency.

The ISACA Crossword Puzzle 1/03

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



Across: **1 disclosing of knowledge;** 10 harvest; 13 away; 14 the pitcher's training ground; 16 former Japanese politician; 17 therefore; 18 international juvenile reunion; 19 Japanese coin; 20 river in Italy; 21 allow; 23 cousin (ger); 25 circle; 26 Greek goddess; 27 oriental calculator; 29 southeast; 30 article (it); 31 technical sub-committee 33 entered (sp); 34 Roman greeting; 35 near; 36 preposition; 37 barrier; 38 camphor-like substance; 42 concerned with bodies in equilibrium; **45 entrusted with secrets; 48 careful;** 49 terrible; 51 thing (lat); 53 auto plate from Southern Switzerland; 54 two equal vowels; 55 sung poem; 56 never ending; 60 confused New York Mets; 62 former princess of Wales; 63 United Nations; 64 signal; 65 festive occasion; 66 mother of Kriemhild; 67 of pre-German origin; 69 the international norm abbreviation stands on its head; 70 former Czechoslovakian auto plate; 71 town in North Africa; 72 own person (lat); 73 bone (fr) 74 Gaugin's lover in Tahiti, if doubled; 76 going by; 78 smallest; 80 spice; **81 uncovering**.

Down: 1 means of transport; 2 is (lat); 3 delicate flower; 4 short form of Edward; 5 unless; 6 auto plate from Turkey; 7 intervene; 8 bringing up; 9 otherwise; 10 Royal women (abb); 11 in (fr), 12 difficult question (pl); 15 character; 18 legendary British knight; **20 data protection;** 22 not in the West; 24 Trans South Asia; 28 auto plate from Switzerland's capital; 32 big meeting (pl); 34 approach; 38 rodent; 39 metal; 40 high density test (abb); 41 long naval haul (abb); 42 British knighthood; 43 coal product; 44 news; 45 university grade potential (pl); 47 narcotic plant; 48 result (pl); 50 put asunder; 52 do as if; 57 European Bank Loan; 58 "I aging", very much confused; 59 article (it); 61 island in the Lake of Constance; 68 oil product firm; 69 capital of Norway; 71 nutrient; 75 Old System Revival; 76 auto plate from Poland; 77 European Community; 79 it (ger).

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, CH-8135 Langnau a/A bis 1. April 2003. Wiederum ist für Tüftler ein „Watson"-Detail versteckt. Lösungen werden auch entgegengenommen unter der Adresse mbretscher@kpmg.com.

Lösungswort 5/02:
Wandtafel

Waagrecht: 2 Plueschtiere; 9 KO; 11 Oese; 13 ie; 14 Alb; 15 R(e)x; 16 Verbalattacke; 22 kosen; 23 Lt; 24 RRR; 25 EB; 27 St; 28 Rad; 29 Troja; 30 If; 32 Hel; 33 Aval; 34 Ei; 35 Lee; 37 on; 39 *Schulen*; 40 Samt; 41 aah; 43 home; 44

Kredit; 46 Relikt; 48 *Beamer*; 49 Kosovo; 50 SRGI; 52 hin; 54 Asen; 55 Motoren; 56 er; 57 ten; 58 pp; 59 ajar; 61 tía; 62 da; 64 Angel; 65 ces; 67 FI, 68 re; 70 les; 72 EK; 74 Buden; 75 *Selbststudium*; 81 Den; 82 oe; 85 Mann; 85 el; 86 *weiterbilden*.

Senkrecht: 1 *Workshop*; 2 PS; 3 lever; 4 ear; 5 CIA; 6 *Hellraumprojektor*; 7 Ist; 8 rear; 9 Klee; 10 Ob; 12 Exoten; 14 AK; 17 Enak; 18 BH; 19 Atolle; 20 Traenke; 21 cri; 26 Brett; 29 TVHO; 31 Fladen; 33 acht; 36 Emir; 38 Halon; 40 Semit; 41 aesend; 42 HIV; 45 Rah; 46 Rose; 47 Kompass; 48 Bier; 49 Kater; 60 stages; 51 Gral; 53 *Training*; 56 eifern; 60 Zebu; 63 All; 66 Summe; 69 Esel; 71 Ebbe; 73 ad; 76 En; 77 Tat; 78 *Ueb!*; 79 Ill; 81 de; 84 an.

Es wurden mehr als 5 richtige Lösungen eingesandt, womit eine Auslosung stattfinden konnte. Gewinnerin ist Marina Müller. Herzliche Gratulation zur Gutschrift von Fr. 50 für Bezüge aus dem ISACA-Bookstore!

Der Watson-Jackpot ist erstmals geleert! Marc Bucher (wohl „SORT-Spezialist“) hat die versteckte Einzelheit richtig festgestellt. Nämlich, dass bei der Fragestellung senkrecht 6 vor 5 abgefragt wird. Bravo, damit gewinnt er US$ 100 in Form von Gutschrift für Bezüge aus dem ISACA-Bookstore! Für das nächste Rätsel sind wiederum US$ 50 im Watson-Jackpot.

News aus den Interessengruppen

Neue Interessengruppen

Wir planen, neue Interessengruppen zu gründen. Als mögliche Themen sind vorgeschlagen:

- IG Continuous Auditing
- IG e-security (z. B. Attack and Penetration, e-defense, e-security Architecture)
- IG Archivierung (Aktualisierung der Arbeiten der ehemaligen IG Aufbewahrung)
- IG ??? Anregungen für weitere IGs nimmt Rolf Merz gerne entgegen.

IG e-business

Leitung a.i.:
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@eycom.ch

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 Anwendung von COBIT

Leitung a.i.
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 6679
Fax. +41 58 286 6827
rolf.merz@eycom.ch

Die IG soll reaktiviert werden. Dazu werde ich die bisherigen IG-Mitglieder anschreiben. Weitere Interessenten melden sich bitte bei Rolf Merz.

IG Outsourcing/ Insourcing

Ueli Engler
KPMG Fides Peat
Badenerstrasse 172
8004 Zürich
Tel. +41 1 249 26 16
uengler@kpmg.com

Letzte Sitzung: Jean-Pierre Brenn wechselt seine Stelle und muss deshalb das Szepter bereits weitergeben. Ueli Engler hat den Stab übernommen und sucht einen Termin für die nächste Sitzung.
Mögliche Themen:

- Kontinuität des Insourcers
- Abhängigkeit vom Insourcer (Konkurs)
- Überarbeitetes Rundschreiben EBK
- Fernwartung, etc.

Nächste Sitzung: Offen. Interessenten melden sich beim Vorsitzenden.

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@eycom.ch

Letzte Sitzung: 15. Januar 2003, EY Zürich
Traktanden:

- Organisatorisches
- Referenzmodell und Metadaten
- Kontrollziele/Risk Matrix
- Diverses

Nächste Sitzung: Ende Januar/Anfang Februar 2003, der genaue Termin wird mittels e-mail koordiniert und kommuniziert.

IG SAP R/3

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

Letzte Sitzung: Donnerstag, 14. November 2002, bei PWC, Zürich
Traktanden:

- ACL/Berechtigungen wie prüfen (Hr. Appl., SNB)
- Qualitätsprüfungskonzept im SAP (Hr. B. Bolli, CCSAP BAIT)
- Im SAP das Risk Assessment Tool RAT einsetzen (Hr. A. Hilsbos, PWC)
- Neues vom Jahresmeeting SAP-AK's (H.J. Stritter, EDV-Audit-Consult)
- Übertragung von SAP Walldorf (M. Galli)
- SAP und AIS AUDITool News, Erfahrungen und Tips (alle)

Nächste Sitzung: Termin noch offen. Interessenten melden Sich bitte bei der IG-Leiterin.

DACH-News

D: Aktivitäten des German Chapter

Ein weiteres Jahr der Vorstandsarbeit ist nun beinahe vorüber und in Kürze steht wieder die Mitgliederversammlung des ISACA German Chapter an. Diese wird am 7. März 2003 im Hilton Hotel in Frankfurt am Main stattfinden. Der Vorstand möchte alle Mitglieder hierzu ganz herzlich einladen und hofft auf eine rege Teilnahme. Wie in den Vorjahren wird allen Mitgliedern noch eine entsprechende schriftliche Einladung per Post zukommen. Bis dahin wird der Vorstand weiter aktiv den Verein vorantreiben.

Nach den Feiertagen hat der Vorstand längst wieder die Arbeit aufgenommen und sich am 24. Januar 2003 zu einer Vorstandssitzung vor der Mitgliederversammlung 2003 getroffen. Weiterhin sind wir mit der Vorbereitung der Mitgliederversammlung, aber auch mit den Vorbereitungen auf unsere erstmalige Präsenz auf der CEBIT in Hannover beschäftigt. Dort wird sich der ISACA als Berufsverband präsentieren und allen Interessierten Rede und Antwort stehen, um unsere Bekanntheit in der breiten Öffentlichkeit zu verstärken. Auf eine rege Unterstützung unserer Mitglieder hoffen wir. Auch laden wir alle Mitglieder ein, einfach einmal bei ihrem Berufsverband auf der CEBIT vorbeizuschauen.

Wer weiteres Interesse an aktuellen Nachrichten hat, Seminare sucht oder *NewsLetter*-Artikel von Mitgliedern des German Chapter in elektronischer Form haben möchte, findet dies alles auf unserer sich ständig weiterentwickelnden Website unter www.isaca.de.

Abschließend möchten wir wieder einmal alle diejenigen Mitglieder ansprechen, die interessante Projekte oder auch wissenschaftliche Themen bearbeiten oder bearbeitet haben. Schreiben Sie doch einfach einmal einen Artikel für den *NewsLetter* und lassen Sie andere auch ein wenig an Ihren Praxiserfahrungen oder dem erworbenem Wissen teilhaben. Wenn Sie Fragen dazu haben sollten, können Sie das Vorstandsmitglied Ingo Struckmeyer jederzeit gern kontaktieren (ingo.struckmeyer@comdirect.de). Sie werden sehen, es ist gar nicht so schwer, einen interessanten Artikel zu schreiben und kann auch Spaß machen. Allen Autoren des letzten Jahres möchten wir an dieser Stelle nochmals für ihre wirklich gelungenen Artikel danken.

Vorstand German Chapter
i.A. Ingo Struckmeyer

CH:

Voranzeige: EUROCACS 2004 in der Schweiz

Entgegen unserer Erwartungen und entsprechenden Kommunikation an der letzten Generalversammlung wurde Zürich als Ort der Durchführung für die EUROCACS 2004 gewählt. Das freut uns natürlich riesig! Aufgrund unserer Erfahrungen aus der Konferenz 1999 wissen wir, dass es einiges zu organisieren und abzuklären gibt. Freiwillige Helferinnen und Helfer sind deshalb gesucht! Meldungen nimmt vorläufig die Redaktion entgegen. Derzeit prüfen wir übrigens Alternativen für den Durchführungsort. Datum der Konferenz: ca. Ende März 2004.

Voranzeige: GV 2003 in Bern

Am 28. März 2003 findet in Bern wiederum die Generalversammlung des Switzerland Chapter von ISACA statt. Traditionsgemäss gibt es vor der eigentlichen GV ein Fachreferat. Die Einladung an alle Mitglieder wird demnächst versandt.

Dieser Anlass ist immer wieder eine gute Gelegenheit, Kolleginnen und Kollegen zu treffen sowie zu einem Fachthema Neues zu erfahren! Deshalb: blockieren Sie bitte schon heute den Termin in Ihrer Agenda! Wir freuen uns auf ein zahlreiches Erscheinen.

CISA: Wir gratulieren nochmals!

Folgende Kandidaten haben die CISA-Prüfung 2002 erfolgreich bestanden (aufgeführt sind nur die Kandidaten, welche das Einverständnis zur Freigabe ihres Resultats gegeben haben):

Armin Suter
Bruno Küng
Cyril Edouard Hauppert
Daniel Brunner
Daniel Heimberg
Daniel Städeli
Elias Schibli
Frank Stäubli
Heino P. Kronenberg
Heinz Dürr *
Heinz W. Sommer
Huey Kein Tan *
Iris Gjinovci
Jakob Kaufmann
Josef Siman
Lothar Gramelspacher
Marc Zweiacker
Markus Hug
Martin Dietrich *
Martin Perewusnyk
Martin Sibler
Michael Wegmann
Michel Patcas
Oscar Candrian
Peter A. Nussbaumer
Peter J. Kunz
Reto Bürgi
Rolf Oberle
Roman Malovecky
Rüdiger Scheibl *
Stefan A. Ulmer
Stefan Käser
Stefan Salzmann
Stephan Vedani
Tom Schmidt *
Ulrich Amberg

* Top Scorers! Die ersten drei Ränge, bezogen auf den Prüfungsort Zürich. Im zweiten und dritten Rang gab es jeweils zwei Kandidaten mit gleicher Punktzahl.

32 der 35 Teilnehmer/Innen des CISA-Kurses haben bestanden. Das ist (schon wieder) ein Rekord: 91,4 % haben bestanden! Weltweit haben „nur“ 51 % bestanden. Demnach auch (schon wieder) eine Gratulation an den CISA-Kursleiter Peter Bitterli!

CISA: Entwicklung von Multiple-Choice-Fragen

ISACA International sucht für das CISA Review Manual 2004 Personen, welche neue Multiple-Choice-Fragen in Englisch entwickeln. Interessenten wenden sich bitte in Englisch an:
Elia Fernández Torres, CISA
Manager-Certification Study Program And Educational Development
Information Systems Audit and Control Association
3701 Algonquin Road Suite 1010,
Rolling Meadows, IL 60008, USA
Phone: +1.847.253.1545 ext.484
Fax: +1.847.253.1443
E-mail: efernandez@isaca.org

Eine Revisionsassistentin versuchte bei der Informatikprüfung den dreifachen Lutz.
Sie verhakte sich tüchtig, drehte sich viermal und fiel schliesslich auf ihren Verputz.
Sie ging ins Büro, fluchte und rauchte.
Die Worte, die sie dabei gebrauchte,
Ja die, meine verehrten Damen und Herren, die fallen doch unter den Datenschutz.

There was a young lady auditor who was living in Rust
Who put all her money into an information technology trust
She was duly deceived
And not very relieved
When her investment was lost and again go working she must.

Veranstaltungen

Securing and Auditing Windows 2000 Server	17.–20. März 2003 London, 4 Tage, MIS
Brandschutz im Wandel	20. März 2003 Zürich, 1 Tag, SSI
EuroCacs	23.–26. März 2003 Amsterdam, 4 Tage, ISACA
Defense Lab – Live Hacking, Angriffstechniken, Gegenmassnamen	1./2. April 2003 Karlsruhe, 2 Tage, Secorvo
Sichere E-mail-Kommunikation	8./9. April 2003 Karlsruhe, 2 Tage, Secorvo
PKI – Public Key Infrastructure	6./7. Mai 2003 Karlsruhe, 2 Tage, Secorvo
PKI für Fortgeschrittene	8. Mai 2003 Secorvo, Karlsruhe
Informationstechnologie für Wirtschaftsprüfer und Finanzrevisoren	12.–15. Mai 2003 Zürich, 4 Tage, ISACA CH
IT Audit School	12.–16. Mai 2003 London, 5 Tage, MIS
Securing and Auditing Windows 2000 Server	13.–16. Mai 2003 London, 4 Tage, MIS
Lotus Notes Security	10.–21. Mai 2003 Secorvo, Karlsruhe
Neuigkeiten in der Überwachung von Zahlungs- und Effektenabwicklungssystemen	18. Juni 2003 Bern, 1 Tag, ISACA/Kammerseminar
E-Biz Security Lab	8.–10. Juli 2003 Rapperswil, 3 Tage, ISACA CH
SAP R/3 Workshop für Wirtschafts- und Informatikprüfer	12.–15. August 2003 Stuttgart, 4 Tage, ISACA CH
Internet Security Lab	20.–22. August 2003 Zürich, 3 Tage, ISACA CH
Application Security Lab	27.–29. August 2003 Zürich, 3 Tage, ISACA CH
Internet Security Lab	5.–7. November 2003 Zürich, 3 Tage, ISACA CH
Application Security Lab	12.–14. November 2003 Zürich, 3 Tage, 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

Datenschutzbeauftragter des Kantons Zürich
IT-Sicherheitsberatung und -Revision
Andrea Carlo Mazzocco, CISA
Kurvenstrasse 31
CH-8090 Zürich
Tel. +49 1 259 46 08
Fax. +49 1 259 51 38
andreacarlo.mazzocco@dsb.zh.ch
www.datenschutz.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

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. Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
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
Georgios Safaridis
D-Hamburg
georgios_safaridis@web.de

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 bank AG
Internal Audit
Pascalkehre 15
25451 Quickborn
Tel. +49 4106 704 1233
Fax. +49 4106 704 1990
ingo.struckmeyer@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-Koordinator
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 1 285 69 36
Fax. +41 1 285 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
Bankstr. 1
8570 Weinfelden
Tel. +41 71 626 64 61
Fax. +41 71 626 63 60
p.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-Koordinator
Thomas Bucher
Ernst & Young Ltd
Badenerstrasse 47
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 36 88
thomas.bucher@eycom.ch

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
PricewaterhouseCoopers
Nordstr. 15
8035 Zürich
Tel. +41 1 630 27 82
Fax. +41 1 630 27 55
monika.josi@ch.pwcglobal.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@eycom.ch

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
Rentenanstalt/Swiss Life
General Guisan-Quai 40
Postfach 4338
8022 Zürich
Tel. +41 1 284 31 07
Fax. +41 1 284 47 33
bruno.wiederkehr@swisslife.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch