Information Systems Audit and Control Association

News Letter

Nr. 64, Juni 2003

Thema Katastrophenfallplan

Switzerland Chapter
Germany Chapter
Austria Chapter

© 3.7.2003

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: 1020 Exemplare

Nächste Ausgabe (Thema: Zahlungssysteme): September 2003, Redaktionsschluss: 29. August 2003

Inhaltsverzeichnis

Editorial 4

Katastrophenfallplan – Prüfung von Business Continuity Planning und Katastrophenvorsorge bei IT Outsourcing von Banken 6

Katastrophenfallplan – Den Krisenfall simulieren 10

Katastrophenfallplan – Disaster Recovery bringt mehr IT Sicherheit 13

Katastrophenfallplan – Einige Tipps zur Notfallplanung 16

Datenschutz – Marktwirtschaftlicher Datenschutz 19

Datenschutz – Die Modernisierung des Datenschutzes und die Rolle des eidgenössischen Datenschutzbeauftragten 24

Express Line 27

The ISACA Crossword Puzzle 28

DACH-News 30

Veranstaltungen 33

Germany Chapter 35

Austria Chapter 36

Switzerland Chapter 37

Editorial

Der „teure“ Katastrophenfallplan

Angesprochen auf die Massnahmen gegen eine mögliche Überflutung (Dammbruch des Sihlsees, der Zürich überfluten würde), erhielt ich denn schon vor Jahrzehnten die Entgegnung: „Wenn der Sihlsee kommt, ist so viel kaputt, dass es auf eine Datensicherung am Zürichberg auch nicht mehr ankommt. So ein Katastrophenfallplan ist erstens teuer und zweitens nützt er insbesondere deshalb nichts, weil die Wirklichkeit sowieso anders ist, als es der Plan vorsieht.“ Ist dies so?

In einer Risikomatrix sind Katastrophen im Feld rechts unten angesiedelt. Typischerweise werden diese Risiken (hohe Tragweite, geringe Wahrscheinlichkeit) entweder in fatalistischer Weise ignoriert oder transferiert, d.h. versichert. Die Möglichkeit der Versicherung wiederum hängt davon ab, ob sich überhaupt ein Versicherer findet, der das Risiko übernimmt. Entweder sind die Prämien enorm teuer oder der Versicherer bietet eine entsprechende Police gar nicht an. „Viel zu teuer“, sagen viele Betreiber. Nochmals: Ist dies so?

Kürzlich nahm ich an einer Tagung bezüglich Informatik und Recht teil. Dabei beeindruckten mich die Ausführungen der Referenten, welche auf die rechtlichen Folgen von Unterlassungen bei Verkauf, Entwicklung und Betrieb von Informatikprodukten hinwiesen. Ich zitiere Dr. Wolfgang Straub, LL.M. und Dozent an der Universität Fribourg im Zusammenhang mit der Thematik von ausservertraglicher Haftung:
„ … Die Schadenshöhe bei IT-Ausfällen hängt oft in erheblichem Mass davon ab, ob der Betroffene auf eine entsprechende Situation vorbereitet war oder nicht … In welchem Mass ein *Disaster Recovery Planning* heute allgemein vorausgesetzt werden kann, hängt … von Art und Grösse des Unternehmens ab. Es handelt sich dabei sozusagen um präventive Schadensminderungspflichten … Um zu belegen, dass alle sich aufdrängenden Schadenverhütungs- und Schadenminderungsmassnahmen getroffen wurden … kann für den Betreiber eines Informationssystems der Nachweis eines aktuellen *Sicherheitskonzepts* und die periodische Überprüfung seiner Einhaltung wichtig sein.“

Sehen wir also einmal von einem Naturereignis wie dem Dammbuch des Sihlsees ab, sondern unterstellen wir, die Katastrophe sei durch einen Dritten ausgelöst worden, zum Beispiel ein von einem Hersteller gelieferter fehlerhafter Temperaturfühler, der letztlich für eine Brandkatastrophe verantwortlich ist. Wenn der Betreiber der IT-Anlage nun glaubt, er könne den Schaden vollumfänglich als Haftpflichtfall dem Lieferanten des fehlerhaften Temperaturfühlers überbinden, kann er gemäss vorstehend zitierter Rechtslage eine böse Überraschung erleben. Wäre ein (allenfalls rudimentärer) Katastrophenfallplan immer noch „viel zu teuer“ gewesen?!

An der gleichen Tagung diskutierte eine Subgruppe der Teilnehmer die Möglichkeiten der IT-Versicherungen allgemein und der IT-Haftpflichtversicherungen im Speziellen. Interessant war dabei zu erfahren, dass amerikanische und europäische Versicherer am Erarbeiten von Versicherungsprodukten sind, welche die Qualität der Sicherheitsvorkehrungen in der Prämienbemessung berücksichtigen. Ist in dieser Situation ein Katastrophenfallplan immer noch „viel zu teuer“?!

Sicher wird es in jedem Fall ein Abwägen von Kosten und Nutzen bzw. der möglichen Kostenersparnis sein. Aber es gilt zu bedenken, dass entgangener Gewinn nur in sehr seltenen Fällen und ein erlittener Imageverlust (infolge Unmöglichkeit der Lieferung während der unmittelbar auf die Katastrophe folgenden Zeit) überhaupt nie entschädigt werden.

Fazit: Der Katastrophenfallplan ist eine günstige Investition.

Max F. Bretscher

Le „coûteux“ plan de secours

Il y a de nombreuses années, je discutais avec un responsable des mesures de secours prévues en cas de rupture du lac de Sihl qui viendrait inonder Zurich. La réponse fut catégorique : « Si le lac de Sihl déborde, il y aura de toute manière de tels dégâts que l'existence d'une sauvegarde des données sur la colline surplombant Zurich ne jouera plus un très grand rôle. Un tel plan de secours est d'une part trop coûteux et ne sert d'autre part à rien car la réalité ne correspondra de toute manière pas aux hypothèses. » D'accord ?

Dans une matrice de risques, les risques se trouvent traditionnellement en bas à droite : grands dommages et faible probabilité de survenance. De tels risques sont généralement soit ignorés, soit transférés par la conclusion d'une police d'assurance. Cette dernière possibilité est elle-même dépendante du marché et de la disponibilité d'un assureur à conclure un tel contrat, souvent lié à des primes exorbitantes. Toujours d'accord ?

J'ai récemment participé à une journée consacrée au droit et à l'informatique. Les exposés traitant des conséquences juridiques de problèmes en cas de vente, développement ou exploitation informatiques m'ont impressionnés. Je cite le Dr Wolfgang Straub, LL.M et professeur à l'Université de Fribourg sur le thème de la responsabilité extracontractuelle :

« La hauteur du dommage en cas d'incidents informatiques dépend souvent dans une mesure considérable du degré de préparation de l'entreprise à une telle situation. (…) La réponse à la question de savoir si l'on peut aujourd'hui exiger d'une entreprise qu'elle dispose d'un *Disaster Recovery Planning* dépend de la taille et du genre d'entreprise. Il s'agit là de mesures préventives correspondant au devoir général de l'assuré de limiter les dommages. Appelé à démontrer qu'il s'est conformé à cette obligation, l'exploitant d'un système informatique pourrait par exemple devoir documenter l'existence d'un *concept de sécurité* actuel et régulièrement testé. »

Oublions le débordement du lac de Sihl et considérons un cas plus banal : un appareil de mesure de la température livré par un fournisseur est défectueux et entraîne un incendie dans l'entreprise. L'exploitant qui imagine qu'il pourra faire couvrir l'ensemble de ses dommages en arguant de la responsabilité civile du tiers pourrait faire une mauvaise expérience. Si l'on se réfère à la citation susmentionnée, une partie du dommage pourrait lui être imputée si une aggravation des dommages peut être imputée à l'absence d'un plan de secours. Un tel plan est-il dans une telle hypothèse toujours trop coûteux ?

Lors du même séminaire un sous-groupe a traité des assurances, en particulier responsabilité civile, dans le domaine informatique. Une tendance intéressante se dessine aux USA et en Europe : de nouveaux modèles de police intègrent dans le calcul du risque, et donc des primes, le degré de sécurité informatique de l'entreprise. Cette sécurité est-elle toujours trop coûteuse ?

Il est clair qu'il faudra toujours effectuer une soigneuse pesée d'intérêts entre les coûts des mesures et les sommes économisées. Mais il ne faudra pas oublier d'intégrer dans cette réflexion le fait qu'aucune assurance ne couvre le manque à gagner ou les dommages de réputation qui peuvent être liés à un sinistre.

Conclusion : un plan de secours peut dans certains cas constituer un investissement avantageux !

Max F. Bretscher

Katastrophenfallplan

Prüfung von Business Continuity Planning und Katastrophenvorsorge bei IT Outsourcing von Banken

1 Ausgangslage

Swisscom IT Services (SCIS) ist ein führender IT Full Service Provider in der Schweiz. Swisscom IT Services baut, integriert und betreibt komplexe, auf die Verarbeitung grosser Datenmengen ausgerichtete, Systeme. Eine der Kernkompetenzen von Swisscom IT Services besteht in der professionellen und sicheren Verarbeitung von Informationen in einem sensitiven Umfeld. Insbesondere von Kunden aus dem Bankenumfeld werden höchste Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der IT gestellt.

In einem Outsourcing Verhältnis zwischen Kunde und IT Provider ist der Ausfall- bzw. Katastrophenvorsorge (Business Continuity Services) eine fundamentale Bedeutung beizumessen. Unternehmenskritische Systeme und Daten müssen im Fall der Fälle schnell und effizient wieder zum Funktionieren gebracht werden können. Die Antwort auf diese Herausforderung lautet Business Continuity Service, eine Dienstleistung, welche professionelle Vorsorgeanalyse (Business Continuity Assessment), den Aufbau einer Vorsorgelösung (Business Continuity Planning), Beratung und Support im Notfall vor Ort (Disaster Capacity Service) sowie Wiederherstellung der beschädigten Infrastruktur (Disaster Recovery Service) umfasst.[1]

Outsourcingverhältnisse können in unterschiedlichsten Ausprägungen und Ausgestaltungen auftreten.[2] Neben der Regelung von Vertragsgegenstand und gegenseitiger Leistungspflichten sind eine ganze Reihe komplexer Sachverhalte wie Gewährleistung, Haftung, Sicherheitsaspekte oder Kontrolle zu vereinbaren. Dabei stellt auch die Frage, wie die verteilten Massnahmen für die Sicherstellung der Business Continuity angemessen zu prüfen sind, eine Herausforderung für interne und externe Prüfer von IT Provider und auslagernder Unternehmung dar.[3]

2 Regulatorische Grundlage

Die Banken als Outsourcingkunden von Swisscom IT Services unterstehen der Aufsicht und den Regulatorien der Eidg. Bankenkommission (EBK). Gesetzgeber und Aufsichtsbehörde messen einem ununterbrochenen, sicheren und vertrauenswürdigen Bankbetrieb – und dabei explizit auch der Bank-IT – eine zentrale Bedeutung bei. Dies hat sich in verschiedenen Vorschriften niedergeschlagen, von denen hier bezüglich Katastrophenvorsorge und Business Contingency näher auf Artikel 44o der Bankenverordnung[4] sowie das Rundschreiben 99/2[5] näher eingegangen werden soll.

Artikel 44o BankV fordert eher generell die Sicherstellung von „Gesetzmässigkeit, Zweckmässigkeit und Funktionieren der inneren Organisation der Bank unter besonderer Berücksichtigung der Überwachung und Kontrolle der Geschäftstätigkeit und Rechnungslegung durch betriebliche Organisationsmassnahmen“. Grundsatz 4 des EBK-RS 99/2 stipuliert, dass Unternehmung (auslagernde Bank) und IT Provider gemeinsame Sicherheitsanforderungen festlegen und ein Sicherheitsdispositiv erarbeiten, das „sämtliche voraussehbaren Notfälle abdeckt“. Die Weiterführung des ausgelagerten Geschäftsbereiches muss möglich sein, auch wenn der IT Provider aus irgendwelchen Gründen verhindert ist, seine Leistung zu erbringen. Dabei sind die Systeme gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust und technische Fehler durch die Bank und den IT Provider zu schützen. Die Erfüllung dieser Anforderungen sowie die Wirksamkeit der technischen und organisatorischen Massnahmen sind zu überwachen und periodisch zu überprüfen.

Grundsätzlich ist jede einzelne bankengesetzliche Revisionsstelle der auslagernden Bank gehalten, in ihrem jährlichen Bericht[6] zuhanden der EBK Stellung zu nehmen „zur Angemessenheit der elektronischen Datenverarbeitung, vor allem in bezug auf die Organisation, die Sicherheit, die Kontrolle und die hard- und softwaremässigen Ausstattung sowie über die Prüfungen im Zusammen-

hang mit der Einhaltung des EBK-RS 99/2 Outsourcing“. Aus Effizienzgründen wird Prüfung und Berichterstattung beim IT Provider aber nicht von den Prüfern jedes einzelnen Kunden separat durchgeführt. Die Prüfung und Berichterstattung wird von einer von der EBK anerkannten Revisionsgesellschaft vorgenommen,[7] die sich dabei wiederum auch auf die Ergebnisse von internen IT-Prüfern sowohl der auslagernden Bank wie auch von Swisscom IT Services abstützen kann.

3 Das Prüfgebiet Notstands- und Katastrophenvorsorge

Eine Krise[8] wird definiert als ein Ereignis, das den Alltag des Unternehmens destabilisiert und Einflüsse auf die Geschäftspartner und die Umwelt hat. Sie schädigt das Image, das Vertrauen und die Kreditwürdigkeit eines Unternehmens. Unzureichend bewältigte Krisen schlagen sich in Haftungsansprüchen, im Börsenkurs bei kotierten Unternehmen, im Kundenvertrauen und damit in den Absatzzahlen oder in zivil- bzw. strafrechtlichen Konsequenzen für die Organe nieder. Die Bewältigung einer Krise erfordert eine spezielle operative Führung. Anschliessend an den Begriff der Krise könnte Katastrophe als plötzlich hereinbrechendes Ereignis mit schwerwiegende Folgen für Menschen und/oder Sachwerte (Gebäude, Hardware, Applikationen) definiert werden. Eine Katastrophe erzeugt einen dringenden Bedarf an Entscheiden mit weitreichender Tragweite und hat langfristige Nachwirkungen auf die betroffene Unternehmung. Aufgrund von Auslöser und/oder Auswirkung lassen sich verschiedene Arten von Krisen oder Katastrophen unterscheiden:[9]

1. Unfälle: Personenschaden durch Eigen- oder Fremdverschulden;
2. Naturereignisse (Feuer, Wasser, Erdbeben), Brand (verursacht durch menschliches oder technisches Versagen);
3. Deliktische Handlungen: Einbruch (Gewaltsames Eindringen in Gebäude oder Räume), Sabotage (vorsätzliche Beschädigung), Diebstahl (von materiellen oder immateriellen Werten), Spionage (Entwenden von Informationen), Drohung, Erpressung;
4. Ausfall betriebswichtiger Anlagen oder von Sicherheitssystemen (infolge technischem Defekt, Fehlbedienung oder unzureichender Wartung);
5. Abrupte Änderungen des wirtschaftlichen, politischen oder rechtlichen Umfelds.

Gesetzgeber und Aufsichtsbehörden fokussieren bei ihren Anforderungen an die Notstandsvorsorge im Rahmen eines Outsourcing-Verhältnisses deutlich auf den vierten Sachverhalt. In das von Bank und IT Provider gemeinsam zu erarbeitende Sicherheitsdispositiv sind aber natürlich auch die restlichen Aspekte mit einzubeziehen.

4 Prüfungstätigkeiten

Prüfungsschwerpunkte bei Outsourcingkunden

In einem Outsourcingverhältnis sind Leistungspflichten und Verantwortlichkeiten sauber zu definieren bzw. klar abzugrenzen, wobei sowohl Bank als auch IT Provider für die Bewältigung von Krisen und Katastrophen weiterhin selbst verantwortlich bleiben. Der Gesetzgeber fordert von der auslagernden Bank explizit, dass die Weiterführung des ausgelagerten Geschäftsbereiches möglich sein muss, auch wenn der IT Provider aus irgendwelchen Gründen verhindert ist, seine Leistung zu erbringen. Sie muss also Vorkehrungen treffen, um die Geschäftstätigkeit auch bei Ausfällen des IT Providers aufrechterhalten zu können. Das betrifft typischerweise zeitkritische Bankprozesse wie das Handelsgeschäft, die Wertschriftenverwaltung bzw. das ALM, aber auch das Retailgeschäft am Schalter, sollte bei einem Ausfall der IT verzugsfrei weitergeführt werden können.

Aus dieser Anforderung ergeben sich auch die Schwerpunkte für die Prüfungstätigkeit bei der auslagernden Bank: Einerseits Angemessenheit und Aktualität des Business Continuity Assessment, andererseits Wirksamkeit der bankintern implementierten Vorsorgelösung (Business Continuity Planning):[10]

- Entsprechen die vertraglichen Regelungen den Anforderungen des operativen Bankgeschäfts?
- Verfügt der Provider über ein aktuelles Inventar der für die Kunden kritischen Anwendungen?
- Ist die Bewertung der Anwendungen bezüglich Ausfallzeit, Recoverydauer, möglichen Ausweichverfahren auf das operative Bankgeschäft abgestimmt?
- Ist gemeinsam mit dem Provider ein Verfahren definiert worden, wie Krisen zu bewältigen sind?

- Sind die Kommunikationskanäle der Krisenorganisation gegenüber den Stakeholder definiert?
- Bestehen Umgehungslösungen bis zum Recovery des Providers?
- Werden die Umgehungslösungen bis zum Recovery des Providers regelmässig getestet?

Prüfungschwerpunkte beim IT Provider

Bei Ausfällen müssen Hardware, Systemsoftware, Applikationen, Daten oder Infrastrukturen wieder hergestellt werden. Aus dem Business Continuity Assessment der auslagernden Bank resultieren pro System oder Anwendung die maximal zulässige Ausfallzeit und der maximal tolerierbare Datenverlust. Daraus ergeben sich die Anforderungen für vorsorgliche Massnahmen, um in einem Krisenfall den Wiederanlauf des betroffenen Services zu ermöglichen. Regelmässig, in der Regel einmal pro Jahr, sollten ausgewählte Szenarien simuliert werden. Mit diesen Tests werden die Alarmorganisation und das technische Wiederanlaufverfahren (Disaster Recovery Service) verifiziert. Die Tests müssen nachvollziehbar dokumentiert und systematisch ausgewertet werden.

Kontrollziel DS4, teilweise auch DS1 und DS5, von COBIT[11] geben dem Prüfer konkrete Anregungen, welche Anforderungen ein IT Provider zu erfüllen hat. Stellvertretend für viele weitere mögliche sollen hier einige fundamentale Aspekte aufgeführt werden:[12]

- Sind die Anforderungen der Kunden definiert und vertraglich geregelt?
- Verfügt der Provider über ein aktuelles Inventar der für die Kunden kritischen Anwendungen?
- Sind die Anwendungen bezüglich Ausfallzeit, Recoverydauer, möglichen Ausweichverfahren bewertet?
- Ist gemeinsam mit dem Kunden ein Verfahren definiert worden, wie Krisen zu bewältigen sind?
- Wird das Verfahren für die Bewältigung von Krisen regelmässig aktualisiert?
- Unterstützt das Management die Notfallvorsorge?
- Ist zur Bewältigung der Krise eine Organisation definiert?
- Sind Drittanbieter und Lieferanten in die Notfallpläne mit einbezogen?
- Sind die Kommunikationskanäle der Krisenorganisation gegenüber den Stakeholdern definiert?
- Werden die Verfahren und die Organisation in regelmässigen Abständen getestet?
- Werden die Tests systematisch ausgewertet und mit dem Management sowie auslagernder Bank besprochen?
- Wird die Umsetzung der Massnahmen überwacht?

Prüfung der Kommunikationswege und Schnittstellen zwischen IT Provider und auslagernder Bank

Für die Bewältigung von Störungen und Problemen in einem Outsourcing-Verhältnis ist eine konsistente und kanalisierte Kommunikation aller Hierarchiestufen und jedes Verantwortlichen von zentraler Bedeutung. Andernfalls entstehen massgebliche Risiken in Bezug auf die für einen IT Provider wesentlichen Werte wie Zuverlässigkeit und Glaubwürdigkeit.[13] Wesentliche Fragen zur Beurteilung des Kommunikationssystems sind:

- Sind die Kommunikationswege und -medien, die Ansprechpersonen bzw. -instanzen sowie die Stellvertretungen geregelt?
- Sind die Eskalationsstufen definiert?
- Sind die richtigen Instanzen für die Bewältigung involviert?
- Ist die Autorisierung für die Deklaration von verschiedenen Eskalationsstufen definiert?
- Sind die Zuständigkeiten für die Einleitung der nötigen Recovery-Massnahmen bekannt?
- Besteht ein Kommunikationskonzept gegenüber Öffentlichkeit und Presse?

5 Schlussfolgerung

Zentrales Element bei der Prüfung von verteilten Leistungsbeziehungen ist zur Vermeidung von Ineffizienzen eine zwischen den jeweiligen Prüfern abgestimmte Prüfungsplanung und sowie die Verwendung von synchronisierten Prüfprogrammen. Die Prüfer der auslagernden Bank verfügen über das nötige Hintergrundwissen und die erforderliche Legitimation zur Prüfung der bankinternen Prozesse mit den Schwerpunkten Business Continuity Assessment bzw. Business Continuity Planning, während die Prüfer des IT Providers zusätzlich vertieft die Schwerpunkte Disaster Capacity Service sowie Disaster Recovery Service untersuchen.

Für die Prüfung von übergreifenden Prozessen, Kommunikations- und Kontrollsystemen ist hingegen optimalerweise ein Ansatz mit Joint Teams zu wählen, zusammengesetzt aus internen und/oder externen Prüfinstanzen von IT Provider wie auch von der auslagernden Bank. Für eine effiziente, umfassende und konsistente Berichterstattung gegenüber Aufsichtsbehörden und auch gegenüber den jeweiligen Aufsichtsorganen der einzelnen Rechtssubjekte empfiehlt sich die gegenseitige Einsichtnahme und die Durchführung von Peer Reviews.

Business Continuity Services gehört für einen IT Provider zunehmend zum etablierten, aber zugeschnitten auf das aktuelle Kundenbedürfnis optimierbaren, Standardangebot. Praxis und Literatur der IT-Prüfung haben sich bereits seit Jahren mit der Prüfung von Business Continuity und Katastophenvorsorge auseinandergesetzt. Hingegen sind die für die Prüfung von verteilten und komplexen Vertrags- und Leistungsbeziehungen vorhandenen Prüfungsansätze weiter ausbaufähig.

Daniel Wyniger
Georges Lichtsteiner
Swisscom IT Services AG
Bern

Endnoten

1 vgl. http://www.swisscom.com/it/content/DataCenterServices/continuity/index_DE.html

2 vgl. Brändli T. Outsourcing: Vertrags-, Arbeits- und Bankrecht. Bern: Stämpfli, 2001. S. 5f.

3 vgl. Bitterli P. R. Sicherheitsaspekte beim Outsourcing – Aus den Augen, aus dem Sinn? In: ISACA Switzerland Chapter. *NewsLetter* Nr. 57. Februar 2002. S. 5.

4 Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV) vom 17. Mai 1972 (Stand am 30. November 1999)

5 Rundschreiben der Eidg. Bankenkomission (EBK-RS 99/2): Auslagerung von Geschäftsbereichen (Outsourcing) vom 26. August 1999; letzte Änderung am 22. August 2002

6 Rz 20 und 20a Rundschreiben der Eidg. Bankenkommission: Revisionsbericht: Form und Inhalt (Revisionsbericht) vom 21. Oktober 1996 (Stand am 28. Oktober 1999).

7 EBK RS 99/2, Rz. 10 und 44. Vgl. auch die Ausführungen dazu bei Brändli. a.a.O. S. 267.

8 Vgl. Swiss Infosec AG / Zbinden Reto. Informations- und IT-Sicherheit in Theorie und Praxis. Kapitel 6, Teil 4. CD-ROM. 2002.

9 Vgl. Arbeitskreis „Sicherheitsvorkehrungen in Kreditinstituten“. Sicherheit in Kreditinstituten: Handbuch der Arbeits- und Betriebssicherheit. Berlin: Erich Schmidt, 2000. S. 5 ff.

10 Vgl. Arbeitskreis „Sicherheitsvorkehrungen in Kreditinstituten“. a.a.O. S. 162.

11 DS 4 Ensure Continuous Service; DS 1 Define and Manage Service Levels; DS 5 Ensure System Security, COBIT 3rd Edition. Audit Guidelines. IT Governance Institute. July 2000. Weitere wichtige Anregungen liefert z.B. der Code of Practice 1999 (BS 7799-1, Part 1, dt.), Kapitel 11 – Management des kontinuierlichen Geschäftsbetriebs.

12 Für weitere Aspekte vgl. z.B. Kreische K. Anforderungen an die Notfallplanung aus Sicht der MaH. In: Interne Revision. 6. 2001. S. 307 ff. Doemland T. Awareness through auditing, training and testing. In: The Definitive Handbook of Business Continuity Management. Ed. by Hiles. A., Barnes P. 2001, John Wiley & Sons Ltd. West Sussex. S. 247ff. Doughy K. Business Continuity: A Business Survival Strategy. In: Information Systems Control Journal. Volume 1. 2002. S. 2f.; Ferraro A. Auditors Add Value to the Business Continuity Program. In: IS Audit &Control Journal. Volume V. 1998. S. 49. Musaji Y. Disaster Recovery and Business Continuity Planning – Testing an Organization’s Plan. In: Information Systems Control Journal. Volume 1. 2002.

13 Vgl. Beatty G. Emergency response and operations. In The Definitive Handbook of Business Continuity Management. Ed. by Hiles. A., Barnes P. 2001, John Wiley & Sons Ltd. West Sussex. S. 192.

Katastrophenfallplan

Den Krisenfall simulieren

Ein reibungsloser Geschäftsbetrieb ist in einer dynamischen und vernetzten Wirtschaft unverzichtbar. Business Continuity Planning (BCP) ist eine Methode, um die Funktionsfähigkeit der Prozesse zu sichern oder bei Störfällen rasch wieder herzustellen.

Katastrophen kommen in der Regel unerwartet, und meist treten sie im ungelegensten Augenblick ein. Katastrophen beschränken sich nicht auf Ereignisse, welche die Welt erschüttern. Für ein Unternehmen ist bereits der Ausfall der Informationstechnologie ein Disaster, denn er unterbricht innerbetriebliche Prozesse und schneidet den Kontakt zu Kunden und Lieferanten ab.

Die Aufrechterhaltung des Geschäftsbetriebs will geplant sein. Das mag banal klingen, ist aber unabdingbar, will das Unternehmen seine Reputation nicht gefährden. Je anfälliger die Unternehmen für Störungen – seien sie innerbetrieblicher oder externer Natur – sind, desto gründlicher müssen sie sich auf alle Eventualitäten vorbereiten. Und sie müssen auf Unerwartetes rasch reagieren können. Die globale Vernetzung verlangt dabei ein Vorgehen, welches das Unternehmen in seiner gesamten Komplexität erfasst – ein Business Continuity Planning.

Unter Business Continuity Planning – oder kurz BCP – versteht man eine Methode, die es ermöglicht, für Veränderungen im Geschäftsumfeld gewappnet zu sein und diese möglichst zum eigenen Vorteil zu nutzen. BCP beginnt nicht erst, wenn ein Störfall auftritt, sondern umfasst Prävention und Reaktion gleichermassen. Da die Vorbeugung oberste Priorität hat, gilt es, ein Frühwarnsystem auszuarbeiten und Entscheidungskriterien festzulegen, wann gehandelt werden muss.

Disaster einplanen

Die BCP-Methode von PricewaterhouseCoopers basiert auf Simulation. Als erstes wird der Ist-Zustand unter die Lupe genommen. Die geschäftskritischen Prozesse und deren Abhängigkeit von der Infrastruktur, den Systemen und Ressourcen des Unternehmens, aber auch die Beziehungen zu den Geschäftspartnern und die gesetzlichen Auflagen, werden definiert und festgehalten.

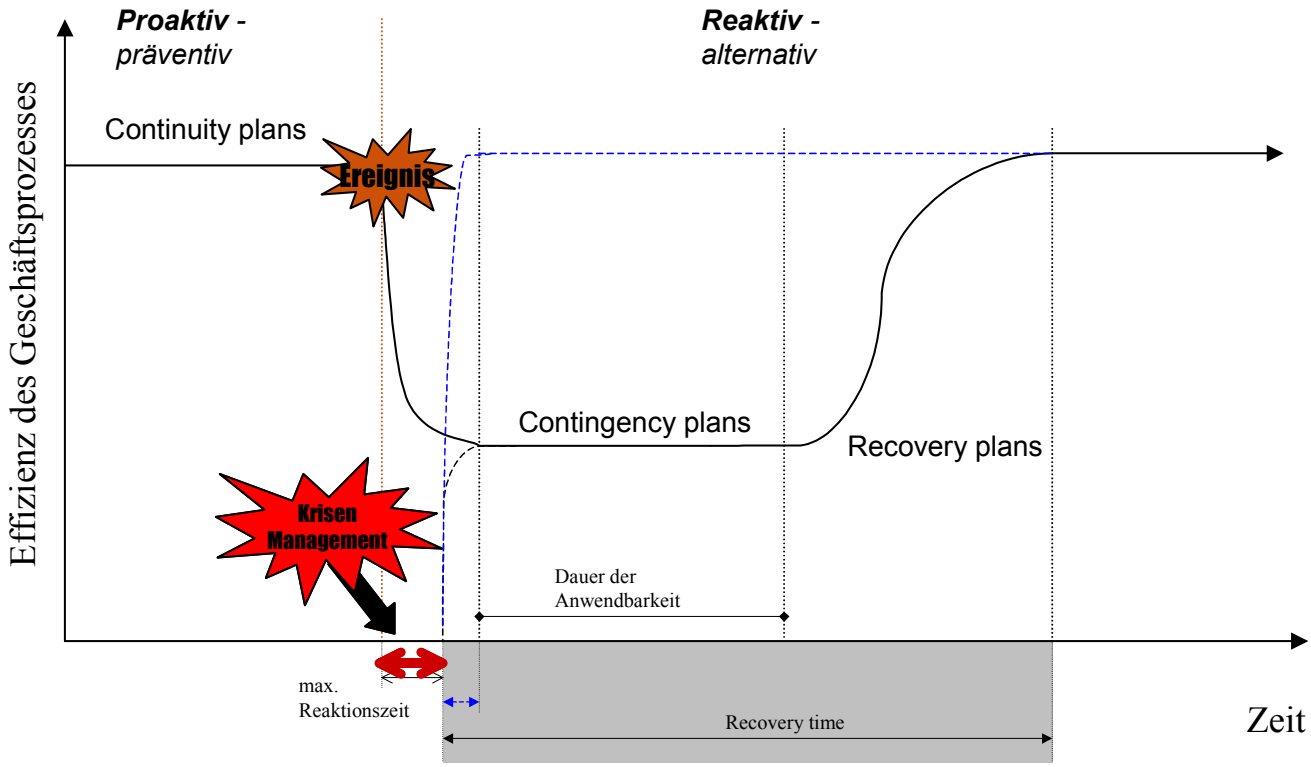
Nach dieser Bestandsaufnahme wird untersucht, wie gravierend sich eine Unterbrechung oder ein Ausfall eines Geschäftsprozesses auswirkt. Ist zum Beispiel ein Imageschaden oder ein finanzieller Verlust zu befürchten oder drohen gesetzliche Einschränkungen, so müssen gezielt vorbeugende Massnahmen eingeleitet werden. Mit anderen Worten: Es muss ein Kontinuitätsplan (Continuity Plan) entworfen werden, um die Stabilität des entsprechenden Prozesses sicherzustellen.

Kommt es dennoch zu einem Störfall, so lassen sich mit Hilfe des Business Continuity Planning die Auswirkungen in Grenzen halten. Da die möglichen Störungen des Geschäftsprozesses in Simulationsmodellen durchgespielt wurden, kann das Unternehmen rasch reagieren. Es kann auf ein geplantes und getestetes Vorgehen zurückgreifen und so das Problem effizient lösen. Eindeutig definierte Verantwortlichkeiten und klare Informationsrichtlinien verhindern eine Verunsicherung der Stakeholder.

Ist ein Prozess einmal unterbrochen, muss das Unternehmen sogleich einen Eventualitätenplan (Contingency Plan) aus der Schublade holen und umsetzen; es muss Massnahmen einleiten, die es erlauben, den Prozess auf einer niedrigeren Effizienzstufe aufrechtzuerhalten. Danach muss alles daran gesetzt werden, möglichst rasch das gewünschte Effizienzniveau wieder herzustellen; der Erholungsplan (Recovery Plan) kommt zum Zuge. Alle Massnahmen müssen regelmässig aktualisiert und getestet werden. Äusserst wichtig ist es, die Mitarbeiter so zu schulen, dass sie die nötigen Schritte rasch und reibungslos umsetzen können.

Vorkehrungen mit grosser Wirkung

Eine entscheidende Rolle spielt der Zeitfaktor. Je rascher ein Unternehmen auf einen Störfall oder eine Katastrophe reagiert, desto eher kann es den Schaden in Grenzen halten. Gerade was die Zeitersparnis anbelangt, hat das Simulationsmodell von PricewaterhouseCoopers einen ent-



scheidenden Vorteil gegenüber den analytischen Verfahren (siehe Grafik), denn die Simulation von Störfällen auf der Grundlage des Alltagsgeschäfts erspart dicke Dokumentationen über Geschäftsprozesse.

BCP ist ein operatives Instrument, um Störfälle oder Katastrophen zu bewältigen. Indem es langfristig stabile Geschäftsprozesse sichert, erhöht BCP die Konkurrenzfähigkeit und bekommt damit auch eine strategische Dimension.

Die langfristigen finanziellen Auswirkungen unvorhergesehener Prozessunterbrechungen lassen sich kaum abschätzen.

Eine rasche Behebung der Störungen ohne konkrete Pläne kann ein Unternehmen sehr viel Energie und finanzielle Substanz kosten. Ein BCP reduziert die Eintrittswahrscheinlichkeit eines Störfalls; geplante und getestete Massnahmen zur Wiederherstellung eines reibungslosen Ablaufs erlauben eine Kalkulation der Kosten, welche die Unterbrechung des Prozesses verursacht hat.

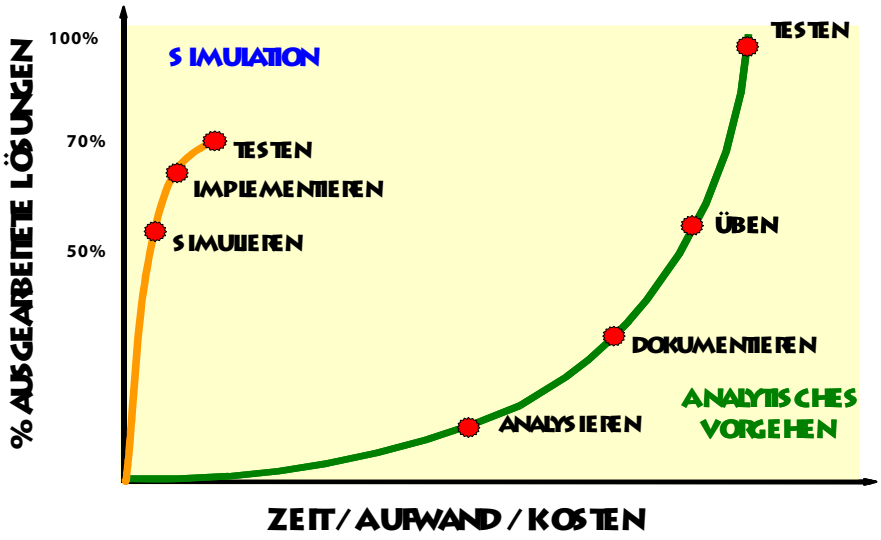
Viele Unternehmen sind sich nicht bewusst, wie stark sie von internen und externen Anspruchsgruppen abhängig sind. Nicht selten ist ein Unternehmen auf einen bestimmten Geschäftspartner angewiesen, um eine Dienstleistung erbringen zu können. Fällt dieser überraschend aus, kann das Unternehmen in eine tiefe Krise stürzen. Um Abhilfe zu schaffen, müssen solche Abhängigkeiten zunächst erkannt werden. Auch dies ist ein Bestandteil des Business Continuity Planning.

Wie wichtig BCP im Zusammenspiel mit den Stakeholdern ist, zeigt sich auch unter dem Gesichtspunkt der wertorientierten Unternehmensführung. Störungen in der Versorgungskette schlagen sich in Lieferschwierigkeiten und in der Qualität der Produkte und Dienstleistungen nieder. Dies wiederum hat Auswirkungen auf Marktanteile und Umsatz, auf das Renommee der Marke und damit auf den Unternehmenswert. Kein Unternehmen kann sich dies leisten. Selbst wenn es zu Prozessunterbrechungen kommt, müssen die Kunden innerhalb der vereinbarten Fristen und in der gewohnten Qualität beliefert werden. Eine schlechte Handhabung von Störfällen kann langfristig nicht nur den Verlust direkt betroffener Kunden nach sich ziehen, sondern – wegen des entstandenen Imageschadens – auch potenzielle Kunden abschrecken. Andererseits wird das Vertrauen der Kunden und überdies sämtlicher Stakeholder erhöht, wenn die Zuverlässigkeit eines Unternehmens auch in aussergewöhnlichen Situationen gewahrt ist.

Wettbewerbsvorteil durch BCP

Instabile Geschäftsprozesse verunsichern auch unternehmensintern. Eine unzuverlässige Infrastruktur erfordert zusätzliche Arbeit und erhöht unnötig den Druck auf die Mitarbeiterinnen und Mitarbeiter. Langfristig wirkt eine solche Situation demotivierend. Sie kann eine erhöhte Fluktuation auslösen und den Ruf des Unternehmens als Arbeitgeber schädigen. Firmen hingegen, welche die Mitarbeiter in die Sicherung der Geschäftsprozesse einbeziehen, erzielen oft den grösstmöglichen Erfolg: Sie erhöhen nicht nur die Qualität der Abläufe im Routine- wie im Ernstfall, sondern werden auch der zentralen Rolle der Mitarbeiter für einen reibungslosen Produktionsprozess gerecht.

Auch für den Umgang mit staatlichen Stellen ist die Aufrechterhaltung des Geschäftsbetriebs von zentraler Bedeutung. Regulatorische Vorgaben zur Qualitätssicherung und zu getreuer Geschäftsführung müssen stets eingehalten werden. Ist ein Unternehmen aufgrund eines Vergehens einmal auf der „Schwarzen Liste“, so ist seine Reputation bei den Behörden und in der Öffentlichkeit angeschlagen. Ein solcher Imageschaden lässt sich, wenn überhaupt, nur mit erheblichem Zeit und Kostenaufwand wieder wettmachen. Ein durchdachtes Business Continuity Planning hilft, einem solchen Reputationsverlust vorzubeugen. Die Ausrichtung der Geschäftstätigkeit nach Geschäftsprozessen und Arbeitsabläufen erhöht die Transparenz und vereinfacht die Qualitätskontrolle.



Die Dynamik der heutigen Wirtschaft bringt ständige Veränderungen des Geschäftsumfelds mit sich. Dies macht laufend neue Anstrengungen nötig, um bestehende Geschäftsprozesse anzupassen und immer wieder neu zu optimieren. Nur wenn die Prozesse in einem Business Continuity Planning festgehalten sind, lässt sich der Nutzen dieser Anpassungen im Vergleich zum ursprünglichen Zustand quantifizieren. Erst die Konzentration auf die kritischen Komponenten zur Sicherung eines Geschäftsprozesses erlaubt eine optimale Allokation von Ressourcen. Mit einem gut ausgearbeiteten BCP gelingt es nicht nur, schneller und besser als die Konkurrenz auf ausserordentliche Situationen zu reagieren, sondern auch Veränderungen im Geschäftsumfeld zum eigenen Vorteil zu nutzen.

Von Felix Sutter
und Patricia Schmutz
PricewaterhouseCoopers
Zürich

Katastrophenfallplan

Disaster Recovery bringt mehr IT-Sicherheit

Die Folgen eines temporären Ausfalls oder dauernden Verlusts businesskritischer Systeme und Daten können fatal sein. Mit Business Continuity & Disaster Recovery Planning werden IT-Risiken kontrollierbar.

Katastrophen sind manchmal von einem Ausmass, dass uns der Atem stockt. Ein anderes Mal passieren sie beinahe unbemerkt, aber zerstören die Existenz der Betroffenen. In der Geschäftswelt ist häufig die Informatik Opfer oder Verursacher von Katastrophen, die den Fortbestand von Unternehmen gefährden.

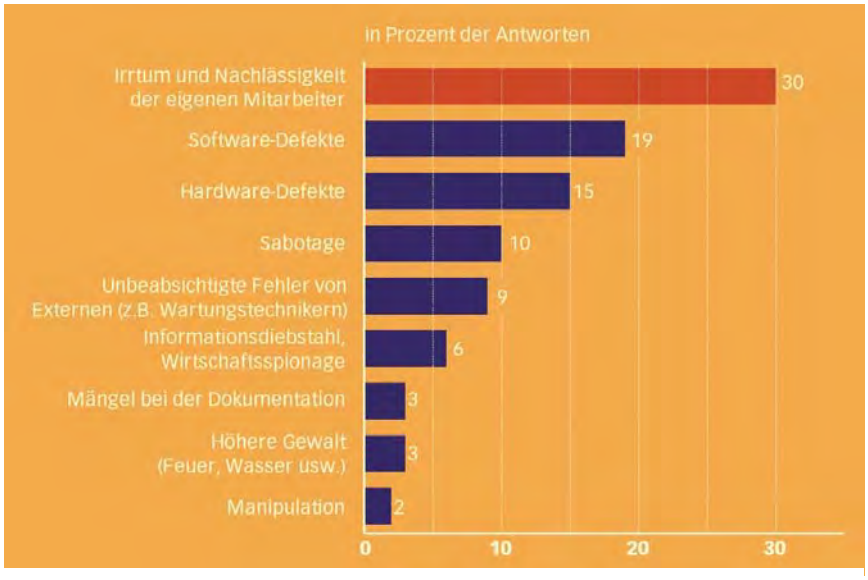
Die Definition einer Katastrophe als jedes nicht vorhersehbare Ereignis, das den normalen Betrieb einer Organisation wesentlich beeinträchtigt, klingt noch nicht alarmierend. Mehr Schrecken verbreiten „richtige“ Katastrophen wie Erdbeben, Brände oder Überschwemmungen. Doch sind es häufig die kleinen Ursachen im Verborgenen, die den Unternehmen grössten Schaden zufügen. So führen Unachtsamkeiten in der täglichen Routine die Liste der Bedrohungen im Urteil von 260 IT-Verantwortlichen in Deutschland an (Grafik 1).

Ob der Mensch, die Technik oder die Natur der Krisenherd ist – ein Ausfall der Informatik kann fatale Folgen haben: die Produktion steht still, die Liquidität sinkt, Kredite können nicht bedient werden, die Reputation des Unternehmens ist gefährdet. Umso beunruhigender ist es, dass gemäss der Studie „IT-Kosten und IT-Performance 2002“ von Ernst & Young mehr als ein Drittel der Schweizer Unternehmen über keine schriftlich formulierte IT-Sicherheitsstrategie verfügt.

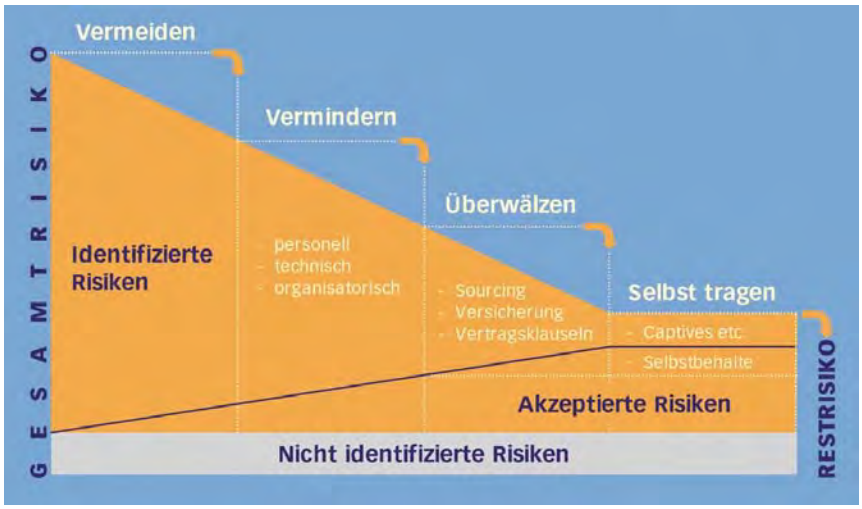
IT-Risiken kontrollieren

Je notwendiger die Informatik aber zur Aufrechterhaltung des Betriebs ist, desto weniger darf ihr reibungsloses Funktionieren dem Zufall überlassen bleiben. Das IT-Risk-Management muss sich dabei laufend auf neue Situationen einstellen: Einerseits werden neue Technologien wie zentrale Datensicherung oder wirksame Zugangskontrollen zum Schutz der IT-Systeme entwickelt, andererseits bergen anspruchsvolle Technologien wie der mobile Zugriff auf Unternehmenssysteme neue Gefahrenquellen.

Kern des Business Continuity & Disaster Recovery Planning ist, IT-Risiken zu erkennen und zu kontrollieren. Business Continuity Planning umfasst sämtliche Strategien und Massnahmen, um die kontinuierliche Verfügbarkeit von Systemen und Informationen sicherzustellen. Disaster Recovery bereitet das Unternehmen auf das Unvermeidbare vor: Die Wiederherstellung und Inbetriebnahme der geschäftskritischen IT-Systeme nach einer Katastrophe. Vorrangiges Ziel ist die Information Security, das heisst die vollkommene oder graduelle Integrität, Konsistenz und Verfügbarkeit von Informationen. Risikostrategien helfen, Risiken zu vermeiden, zu vermindern, auf Dritte zu übertragen oder selber zu tragen. Um Risiken zu vermeiden, werden beispielsweise die Mitarbeitenden auf Gefahren aufmerksam gemacht und entsprechend



Grafik1: Ursachen ungeplanter Ausfälle: Der Mensch ist die grösste Gefahr für die IT
Quelle: KES/KPMG-Sicherheitsstudie 2002, Lagebericht zur IT-Sicherheit



Grafik 2: Stufen des Risikomanagements: «Wie viel Risiko sind Sie bereit zu tragen?» Quelle: Moser, Ulrich: Der IT-Ernstfall – Katastrophenvorsorge; BPX-Edition; Rheinfelden 2003.

geschult. Die verbliebenen Risiken lassen sich durch strikte Zugangsregelungen und -kontrollen zu sensiblen Bereichen weiter vermindern. In einem dritten Schritt können durch die Anbindung an ein zweites Rechenzentrum oder durch den Abschluss spezieller Versicherungen Risiken an Dritte übertragen werden. Risiken mit geringer Eintrittswahrscheinlichkeit werden schliesslich bewusst selbst getragen. So wird das Gesamtrisiko in vier Schritten auf ein akzeptables Restrisiko reduziert (Grafik 2). „Pay or pray“ lautet die Entscheidungsformel für den Umgang mit IT-Risiken.

Drei Stützen im Notfall: Menschen, Prozesse und Technologien

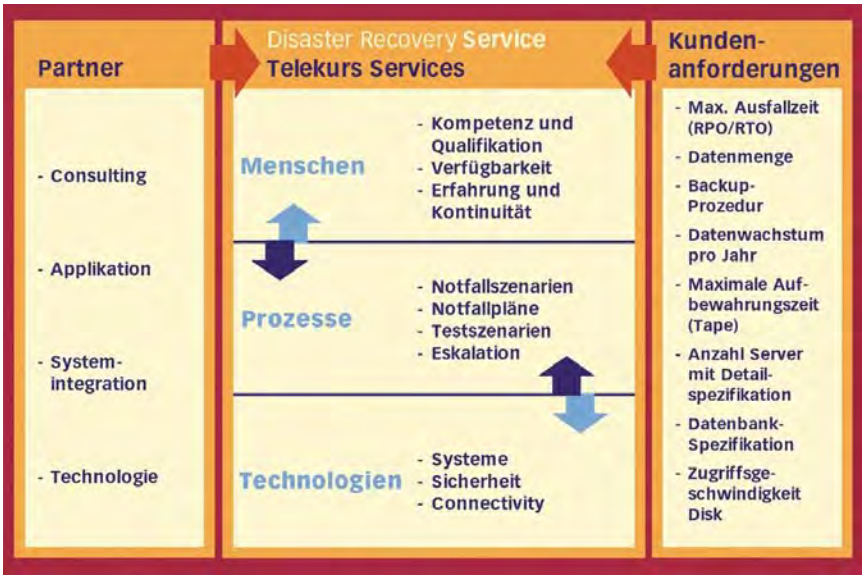
Noch längst ist nicht überall ein systematisches IT-Risk-Management implementiert. Statt Vorkehrungen für den Notfall zu treffen, hofft man, dass dieser nicht eintritt. Doch ein positiver Trend ist erkennbar: Laut Meta Group haben die Global-2000-Unternehmen den Anteil von Disaster-Recovery-Massnahmen am IT-Gesamtbudget in den letzten vier Jahren nahezu verdoppelt. Auch die Rechtslage für den Umgang mit IT-Risiken ist eindeutig: So tragen gemäss Art. 754 Aktienrecht Verwaltungsrat und Geschäftsleitung die undelegierbare Verantwortung für das reibungslose Funktionieren der IT. Andere Normen wie Datenschutz- und Bankengesetz, Versicherungs- und Obligationenrecht sowie weitere Regelwerke wie Basel II, ISO/IEC 17799 (SN 17799) oder Rundschreiben der Eidg. Bankenkommission stärken diese Position. „Best Practice“ bedingt systematische Führungsmethoden und spezialisierte Partner, die ein perfektes Zusammenspiel von Menschen, Prozessen und Technologien ermöglichen (Grafik 3):

Menschen,

- die über die erforderlichen Kompetenzen, Qualifikationen und Erfahrungen verfügen,
- die geschult, zuverlässig und engagiert sind, so dass sie selbst als Gefahrenquelle „entschärft“ werden,
- die im Schadensfall richtig handeln.

Prozesse,

- die helfen, Gefahrenquellen zu erkennen und zu beseitigen,
- die im Notfall rasch greifen, damit Schlimmeres verhindert wird,
- welche die Handlungsfähigkeit der Unternehmung in jeder Situation sicherstellen.



Grafik 3: Menschen, Prozesse, Technologien: Fortschreitende Spezialisierung erfordert neue Partner.

Technologien,

- die unter allen Bedingungen zuverlässige Systeme, korrekte Daten und stabile Kommunikationsverbindungen garantieren.

Gemeinsam mit Consultants, welche die Risikoidentifikation und -bewertung unterstützen, Applikations- und Technologieexperten sowie Systemintegratoren wird die geeignete Disaster-Recovery-Lösung entwickelt und implementiert. Dann entspricht das Zusammenspiel von Menschen, Prozessen und Technologien auch im Notfall den spezifischen Kundenanforderungen.

Von „cold“ bis „hot“: Spürbar mehr Sicherheit

Ein mehrstufiger Prozess stellt sicher, dass alle Risiken erkannt und Vorkehrungen für den Katastrophenfall getroffen werden. So findet das Unternehmen schnellstmöglich zum Normalbetrieb zurück.

1) Risk-Management-Strategie: Risiken werden nach Wahrscheinlichkeiten und Folgen bewertet und alle Strategieoptionen von der Vermeidung bis zum Selbsttragen geprüft.

2) Prävention: Für die einzelnen Katastrophenszenarien werden Vorkehrungen evaluiert, um das Gesamtrisiko beziehungsweise die Einzelrisiken spezifischer Systeme auf ein akzeptables Mass zu reduzieren.

3) Kommunikation und Eskalation: Pläne und Prozeduren regeln das Verhalten im Katastrophenfall, wenn nur wenig Zeit zum Überlegen bleibt und Fehlentscheidungen die Schadensfolgen um ein Vielfaches erhöhen. Eindeutige Zuständigkeiten, Kommunikationswege und Stellvertretungen werden definiert, Abläufe getestet, Ausweichmöglichkeiten, Ersatzbeschaffungs- und Backup-Regelungen für den Ernstfall getroffen.

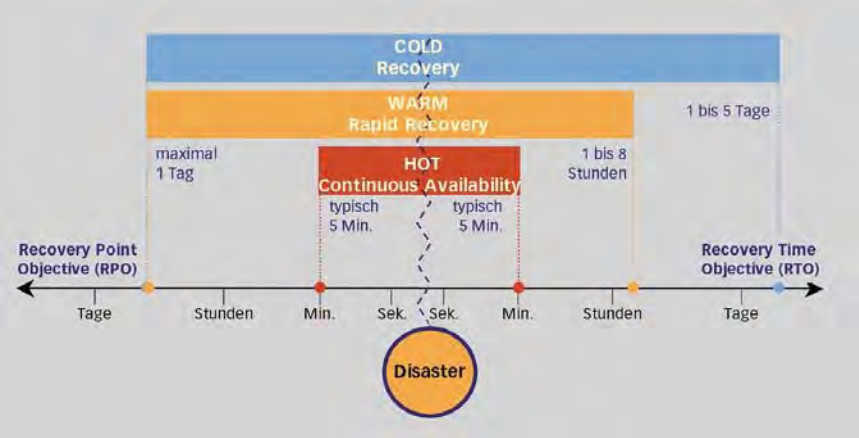
4) Datenzugriff und Wiederherstellung: Regelmässige Backups und/oder Spiegelung der Daten in einem örtlich getrennten Rechenzentrum erlauben es, die Daten im Notfall sicher und integer wiederherzustellen. Es ist zu definieren, bis zu welchem Zeitpunkt vor Eintritt des Disasters korrekte, in sich konsistente, Daten vorliegen müssen. Dieses Recovery Point Objective (RPO) fällt nicht zwingend mit dem Schadenseintritt zusammen, sondern ist der Zeitpunkt der letzten vollständigen Backup- oder Replikationsprozedur. Zusätzlich ist das Recovery Time Objective (RTO), die Zeitspanne, innerhalb welcher der Daten- und Systemzugriff wieder möglich sein muss, festzulegen. RPO und RTO ergeben die maximal akzeptable Ausfallzeit.

5) Notfallarbeitsplätze: Es werden Arbeitsplätze eingerichtet, um im Notfall die wichtigsten Businessprozesse aufrechtzuerhalten. Ausserdem können diese für Testzwecke genutzt werden.

6) Rückführung in den Normalbetrieb: Nach dem Disaster erhält der Kunde Support beim Wiederaufbau des Rechenzentrums und der betroffenen IT-Systeme, um möglichst rasch und mit geringen Schadensfolgen den Normalbetrieb aufnehmen zu können. Eine Schlüsselrolle kommt dabei dem planmässigen, idealerweise geprüften und zertifizierten, Herunterfahren der Notfalllösung und dem Hochfahren der wiederhergestellten IT-Systeme zu.

Anhand dieser individuellen Zielwerte für Datenverlust und Ausfallzeit wird die optimale Disaster-Recovery-Lösung aus drei aufeinander aufbauenden Varianten gewählt (Grafik 4):

- Cold „Recovery“: Daten werden ausserhalb des Hauptstandorts an einem zweiten Standort gesichert. Im Notfall werden Ersatzsysteme bereitgestellt, zum Beispiel über Serviceverträge mit Hardware-Lieferanten. Die Ausfallzeit kann mehrere Tage betragen, die letzten aktuellen Daten stammen vom Vortag. Diese Variante ist vor allem für historische Finanzdaten sowie File- und Printserver-Systeme geeignet.



Grafik 4: Unterschiedliche Anforderungen an die maximale Ausfallzeit: «Wie lange darf Ihre IT ausfallen?»

■ Warm „Rapid Recovery“: In einem Ausweichrechenzentrum werden betriebsbereite IT-Systeme analog zu den Produktivsystemen konfiguriert und im Schadensfall manuell in Betrieb genommen. Die Datensicherung erfolgt durch regelmässige Backups. Notfallarbeitsplätze stehen bereit. Die aktuellsten Daten sind vom Vortag, der System- und Datenzugriff ist in weniger als 24 Stunden möglich. Diese Variante empfiehlt sich für Office-Umgebungen und Auftragsbearbeitung.

■ Hot „Continuous Availability“: Laufende Systeme in einem Ausweichrechenzentrum ermöglichen das rasche Umschalten vom Hauptstandort. Sämtliche Daten werden ständig online gespiegelt, das Recovery Point Objective wird nur von der Verzögerung der Replikation bestimmt. Dies stellt sicher, dass die Ausfallzeit nur wenige Minuten beträgt. Diese Variante ist für businesskritische Handels- und Transaktionsdaten ratsam.

Return on Security

Risk-Strategie und Recovery-Variante sind nach ihrem „Return on Security“ unter Berücksichtigung aller direkten und indirekten Kosten eines Schadensfalles zu bewerten. Den Ausschlag gibt letztlich die akzeptable Ausfallzeit aller oder einzelner Systeme und Daten.

Transparente und leistungsgerechte Kosten für verlässliche Systeme und Daten machen Business Continuity & Disaster Recovery Planning zur kalkulierbaren Investition in die Kontrolle unkalkulierbarer Risiken. Wer den sensiblen Umgang mit kritischen Informationen, eine zuverlässige IT-Infrastruktur sowie den organisierten Wiederaufbau von Systemen als Notwendigkeit versteht, für den sind „pay or pray“ keine Alternativen mehr.

Martin Zeh, Telekurs Services AG Zürich

Nachdruck aus *Netzguide e-Security*, Frühjahr 2003, mit Genehmigung des Autors

Katastrophenfallplan

Einige Tipps zur Notfallplanung

Es gibt einige sehr gute Bücher über Notfallplanung, die umfassend und kompetent über alle Aspekte der Notfallplanung Auskunft geben. Nachstehend sind einerseits aus solchen Büchern, andererseits aufgrund der eigenen Berufspraxis einige Tipps zu zwei Spezialthemen der Geschäftskontinuitätsplanung aufgeführt: zum *Notfallhandbuch* sowie zu *Murphy* (Whatever can go wrong, will go wrong). Diese Tipps erheben keinesfalls den Anspruch von Vollständigkeit, sondern sollen den Leser zum Nachdenken und allenfalls Nachmachen motivieren.

Notfallhandbuch

Ein Notfallhandbuch muss ein praxisgerechtes Führungsinstrument sein. Es enthält die ersten Aktionen, welche durchgeführt werden müssen, so z.B. die Evakuation des Gebäudes, Versorgung der Verletzten, Benachrichtigung von Schlüsselpersonen. Die nachfolgende (unvollständige) Aufzählung kann dabei helfen, ein praxisgerechtes Notfallhandbuch zu erhalten:

1) Einfache Handhabung

Die Informationen müssen schnell griffbereit sein. Dies stellt hohe Anforderungen an Übersichtlichkeit und Transparenz. Erst die Erfüllung dieser Anforderungen garantiert die Akzeptanz durch die Benutzer (Krisenstab, Team-Leiter usw.). Dies erreicht man z.B. mittels Zugriffsmatrizen, Ablaufdiagrammen oder Checklisten für die verschiedenen operationellen Einsatzteams.

2) Nur absolut notwendige Informationen

In Stresssituationen müssen rasch Entscheide getroffen werden. Ein Notfallhandbuch ist daher kein Nachschlagewerk, sondern ein Arbeitsinstrument. Hilfreich sind Entscheidungsmatrizen mit vorbereite-

ten Entschlüssen. Das heisst: Entschlüsse, welche bereits im Vorfeld diskutiert, analysiert und schliesslich gefällt werden, so dass im Ernstfall keine kostbare Zeit mit derartigen Abklärungen vergeudet wird.

3) Übersichtlichkeit und Verständlichkeit

Eine konsequente Visualisierung mit einigen Übersichts-Grafiken und zurückhaltendem Einsatz von Text verbessert die Handhabbarkeit im Notfall.

4) Aktualität ist zwingend

Änderungen im Unternehmen müssen im Notfallhandbuch Rechnung getragen werden. Dies geschieht aber nur, wenn der Nachführungsaufwand des Handbuchs (Zeit und Kosten) akzeptabel ist. Ein modularisierter Aufbau vereinfacht die notwendige Aktualisierung und ermöglicht auch eine rasche Erweiterung mittels neuer Kapitel.

Auch ohne grössere Änderungen im Unternehmen müssen Teile des Plans regelmässig aktualisiert werden: so z.B. die Adress- und Telefonlisten von Schlüsselpersonen resp. sämtlicher Teammitglieder, Verzeichnisse von Lieferanten, Produzenten, Transportunternehmen usw.

5) Bürozeiten von Nicht-Bürozeiten unterscheiden

Viele Notfallpläne gehen davon aus, dass sämtliche von einem Notfall betroffenen Personen in ihren Büros vor Ort sind. Vergessen geht dabei, dass wir in einer Zeit von permanenten Sitzungen leben und daher nur einen Bruchteil der Zeit effektiv im Büro erreichbar sind. Vergessen geht auch, dass wir abends und vor allem nachts nicht im Büro sind (aber in vielen Fällen auch nicht zu Hause!). Man muss also beim Notfallplan analog zum Vorgehen im Brandfall zwischen einer „besetzten" Bürozeit und einer unbesetzten Zeit unterscheiden.

Es gibt übrigens noch eine dritte Zeit (aus meiner Optik die am höchsten kritische Periode überhaupt): die Zeit am Vormittag, wo die Mitarbeiter noch nicht vollzählig anwesend sind, resp. die Zeit, wo die meisten bereits gegangen, aber noch nicht zu Hause angekommen, sind.

Murphy

Die nachfolgende Aufzählung ist eine zufällige Sammlung von typischen Problemsituationen, die bei der Aktivierung eines Plans (Training oder echter Notfall) auftreten können. Es lohnt sich, während der Schulung und bei realistischen Tests diese Fälle bewusst zu provozieren.

1) Entscheidungsfaulheit

Notfallsituationen laufen ab aufgrund der oft chaotischen Gesetzmässigkeiten einer Krise und nicht nach Plan. Dies steht aber im Widerspruch zu den (psychologischen) Verhaltensweisen der Menschen, die dann typische Fehler produzieren. Solche Reaktionen in Notsituationen sind z.B. „Das ist ja nicht so schlimm, wir werden das innert kürzester Zeit im Griff haben." (und die Zeit läuft davon) oder „Das ist ja nicht so schlimm, wir können das selber lösen und auf die Alarmierung verzichten." Generell tendieren viele Entscheidungsträger dazu, länger als im Notfallplan vorgesehen auf bestimmte Reaktionen oder Ereignisse zu warten, obwohl im voraus anderslautende Entschlüsse getroffen wurden. Die dadurch verlorene Zeit ist in der Regel nie mehr aufholbar!

2) Unmöglichkeit, die Teams aufzubieten

Im Zeitalter der Handies basieren viele Alarmierungspläne darauf, dass man Krisenstab und Notfallteams per Mobiltelefon aufbieten kann. Typischerweise sind bei nach aussen sichtbaren Ereignissen (z.B. Grossbrände) die Telefonnetze komplett überlastet oder werden sogar von der Polizei oder anderen Einsatzkräften abgeschaltet resp. sind nur noch für deren Zwecke verwendbar. Im weiteren sind Handies oft nicht dabei, ab- oder stummgeschaltet, so dass die Alarmierung die Zielperson nicht erreicht.

Festnetznummern sind zwar viel zuverlässiger, die gesuchten Mitarbeiter aber nicht am Platz, noch nicht zu Hause oder dort z.B. wegen dem eingeschalteten Telefonbeantworter effektiv nicht erreichbar. Besonders kritisch ist die Übergangszeit nach Arbeitsschluss, wo viele auf dem Nachhauseweg noch in die Bar, ins Restaurant, ins Training oder zu sonstigen Anlässen gehen. Es lohnt sich, einmal eine Alarmie-

rungsübung zu diesen Zeiten durchzuführen.

3) Notfall während einem grossflächigen "Ereignis"

Es ist offensichtlich, dass die Reaktionszeit und vor allem die „Verschiebungszeit" von Teammitgliedern während einer Katastrophe, von der auch andere Firmen resp. Personen betroffen sind, massiv vergrössert werden kann (z.B. Überschwemmung, Sturm, usw.). Vergessen geht, dass tagtäglich in jeder grösseren Stadt Ereignisse stattfinden, welche einen Einfluss auf den Verkehr und damit die erwähnte Verschiebungszeit haben: Fussballmatch, lokaler Feiertag, Feuerwerk, Love Parade, Quartierfest, Velo-Demo, Baustellen (!) usw.

Eine Übung mit dem Ziel, die Teammitglieder an ihren Einsatzort aufzubieten, sollte daher von Vorteil einmal während eines solchen (voraussehbaren und damit für Schulungszwecke vorausplanbaren) Ereignisses stattfinden – die Verschiebungszeiten verdoppeln sich da locker! Dies gilt zwar als unfair, ist aber sehr ernüchternd.

4) Notfall ohne Köpfe

Es ist unbestritten: Es gibt in jeder Firma und bei jeder Krisensituation Schlüsselpersonen, bei deren Anwesenheit alles eine Spur einfacher, schneller und besser läuft. Leider sind diese Schlüsselpersonen in den Notsituationen vielleicht gerade nicht erreichbar oder können nicht innerhalb nützlicher Frist an ihren Einsatzort kommen. Man sollte daher diese Situation üben und z.B. in jedem Team den Teamleiter entfernen (nicht als Beobachter einsetzen, sondern z.B. in ein separates Schulungsszenario entfernen).

Peter R. Bitterli, CISA

Datenschutz

Marktwirtschaftlicher Datenschutz

In immer mehr deutschen Datenschutzgesetzen tauchen Bestimmungen zum Thema Datenschutzaudit auf. Den Anfang machte schon vor fünf Jahren der Mediendienstestaatsvertrag[1], in dessen § 17 ein Datenschutzaudit vorgesehen ist. Danach folgten einige Landesdatenschutzgesetze[2] im Zuge der Anpassung an die Europäische Datenschutzrichtlinie. Auch das Bundesdatenschutzgesetz von 2001[3] enthält eine Regelung zum Datenschutzaudit. § 9a lautet wie folgt: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitenden Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“ Die Vorschrift war im Gesetzgebungsverfahren äusserst umstritten, weil einige betriebliche Datenschutzbeauftragte Bedenken vorgetragen hatten. Im Ergebnis regelt sie unter der Überschrift Datenschutzaudit sowohl die Zertifizierung von IT-Produkten als auch die Auditierung von Datenschutzkonzepten Daten verarbeitender Stellen. Indes: Zur tatsächlichen Einführung von Datenschutzaudits ist nach dem Wortlaut von § 9a ein Ausführungsgesetz notwendig, das einstweilen nicht in Sicht ist. Der Mediendienstestaatsvertrag, der schon vor fünf Jahren ein solches Gesetz in Aussicht stellte, ist hoffentlich kein schlechtes Omen. Auch die Landesdatenschutzgesetze belassen es bis auf Schleswig-Holstein[4] und Mecklenburg-Vorpommern[5] bei einer Ankündigungsnorm. In Mecklenburg-Vorpommern könnte die Landesregierung das Datenschutzaudit nach dem neuen LDSG per Rechtsverordnung einführen, in Schleswig-Holstein ist dies bereits 2001 geschehen[6]. Ein Blick in die deutsche Gesetzgebung zeigt also, dass das Datenschutzaudit im Kommen ist, dass die Gesetzgeber bis auf Schleswig-Holstein bislang aber noch nicht den Mut zum entscheidenden Schritt hatten.

Marktvorteil

Was sind die Gründe dafür, dass überall über Datenschutzaudits nachgedacht wird und mancherorts sogar schon Nägel mit Köpfen gemacht werden? Eine Ursache liegt sicherlich in der Begrenztheit des bisherigen Datenschutzansatzes. Er ist an Kontrolle, Kritik und Beanstandung orientiert, hat also einen deutlichen ordnungsbehördlichen Touch. Die Firmen und Behörden verbinden mit dem Thema Datenschutz folglich eher unangenehme Vorstellungen. Zwar ist das tatsächliche Risiko – vor allem für Privatfirmen – wirklich einmal gründlich kontrolliert zu werden, angesichts der realen Ausstattung der Datenschutzaufsichtsbehörden eher gering. Aber ganz ausschliessen kann man einen Besuch der Datenschutzkontrolleure nie, und das Risiko ist gross, dass dabei Mängel festgestellt werden. Gelangen Informationen hierüber an die Öffentlichkeit, dann ist ein empfindlicher Imageverlust schon vorprogrammiert. Der Datenschutz ist für viele also ein lästiges Thema, mit dem man sich ungern ernsthaft und intensiv auseinandersetzt, das man aber tunlichst nie ganz aus den Augen verlieren sollte. Es ist ein Thema, bei dem man bislang nichts Rechtes gewinnen, wohl aber verlieren kann. Selbst wenn man nämlich das Gesetz ordnungsgemäss umsetzt, bekommt man nichts dafür. Das derzeitige Datenschutzsystem kennt keine Belohnung, keinen Gewinn, sondern allenfalls Verlust[7]. Aus Umfragen[8] ist bekannt, dass die grosse Mehrzahl der Bürger und Kunden auf einen sorgsamen Umgang mit ihren Daten Wert legt. Nicht wenige Firmen hätten durchaus Interesse daran, diese Erwartung mit einem guten Datenschutzkonzept in einen handfesten Marktvorteil umzumünzen. Dazu braucht man ein Instrument wie das Datenschutzaudit, an dessen Ende einer Firma förmlich bestätigt wird, dass bei ihr personenbezogene Daten in guten Händen sind. In unserer Medienwelt muss so etwas kommuniziert werden, zum Beispiel in Form von Auditzeichen und Gütesiegeln. Wenn es speziell um Gütesiegel für IT-Produkte geht, ist noch ein weiterer Aspekt zu berücksichtigen. Seit Jahren ist in der Datenschutzliteratur

anerkannt, dass der Datenschutz allein mit gesetzgeberischen und organisatorischen Massnahmen nicht zu gewährleisten ist. Hinzukommen muss auch eine datenschutzgerechte Gestaltung der Informationstechnik[9]. Mehr noch: entsprechend designte IT-Produkte können sogar zu einer deutlichen Verbesserung des Datenschutzes beitragen. Die Diskussion über solche Privacy Enhancing Technologies (PET)[10] bleibt aber solange akademisch, solange es nicht gelingt, Forscher, Entwickler, Hersteller und Anbieter von Informationstechnik dazu zu bewegen, tatsächlich solche Produkte zu entwickeln und anzubieten. Auch hier könnten sich Produkt-Gütesiegel als der entscheidende Hebel erweisen, der PET zum Durchbruch verhilft. Denn in einer Marktwirtschaft ist nun einmal der Wettbewerb das Mass aller Dinge und PET können nur dann einen Wettbewerbsvorteil versprechen, wenn sie als solche für das Publikum kenntlich gemacht werden. Ohne ein überzeugendes Gütesiegelkonzept, dass das Vertrauen der Kunden verdient, bleiben alle Träume von PET wohl für lange Zeit nur graue Theorie.

Demokratisierung

Audit und Gütesiegel könnten den Datenschutz also marktgängig machen, ihn das lästige Verliererimage vom Wettbewerbsnachteil abstreifen lassen und ihn stattdessen als einen Wettbewerbsvorteil erscheinen lassen, bei dem man nicht nur verlieren, sondern auch gewinnen kann. Diese Rechnung kann freilich nur dann aufgehen, wenn das Thema Datenschutz für die Kunden tatsächlich eine Relevanz hat, wenn es also eine Nachfrage nach Datenschutz gibt. Die konstant hohen Werte, die der Datenschutz bei Umfragen erhält, bedeuten noch nicht automatisch eine hohe Marktnachfrage, aber sie sind ein starkes Indiz [11]. Würden die Kunden bei ihren Kauf- und Investitionsentscheidungen tatsächlich auch die Datenschutzaspekte des Angebots berücksichtigen, so hätte dies vermutlich eine Reihe von Nebenwirkungen, die in Gänze noch gar nicht zu überblicken sind [12]. In jedem Fall wäre damit aber eine Art „Demokratisierung“ des Datenschutzes verbunden, denn er wäre nicht länger nur eine Angelegenheit für Spezialisten, sondern er müsste kommuniziert werden. Die Kunden würden durch ihr Konsumverhalten zurückmelden, welche Art von Datenschutz sie sich wünschen und was sie dafür aufzuwenden bereit sind. Unter der Hand würde sich der Datenschutz, vor allem in den Augen junger Menschen, vom schwer erkämpften, Wirtschaft und Staat täglich aufs Neue abgerungenen Grundrecht zu einem selbstverständlichen Service wandeln, zu einem Teil des Lifestyles, den man sich nicht mehr in Frage stellen lässt. Aber das greift den Dingen vielleicht schon ein wenig voraus. Zurück zum Alltag muss noch kurz die Frage angeschnitten werden, was all diese marktwirtschaftlichen Überlegungen mit der staatlichen Datenverarbeitung zu tun haben. Jedenfalls mehr als man im ersten Moment glauben möchte. Denn im Rahmen der Verwaltungsmodernisierung tritt der Staat zunehmend weniger hoheitlich auf und begreift den Bürger mehr und mehr als Kunden, den es mit gutem Service zu umgarnen gilt. Längst sprechen Verwaltungsmodernisierer von einem begrenzten Wettbewerb der Behörden untereinander, während im Rahmen des Outsourcing der Wettbewerb zwischen staatlichen und privaten Anbietern bereits voll entbrannt ist. Ob es einem gefällt oder nicht, auch im öffentlichen Sektor herrscht zunehmend Wettbewerb und marktwirtschaftliche Überlegungen sind auch dort längst kein Fremdwort mehr [13]. Marktwirtschaftlicher Datenschutz passt also durchaus „in die Zeit“ und Audit und Gütesiegel sind seine adäquaten Ausdrucksformen. Sie sind die Fortsetzung der Modernisierung des Datenschutzes mit marktwirtschaftlichen Mitteln und sie sind die Umsetzung der Erkenntnis, dass ein bloss juristischer, hoheitlicher und ordnungsbehördlicher Datenschutz auf Dauer keine Chance hat.

Praktische Erfahrungen

Erste praktische Erfahrungen mit Datenschutzaudit[14] und Gütesiegeln werden derzeit in Schleswig-Holstein gesammelt. Getreu dem Motto der Ministerpräsidentin, man wolle den Datenschutz als einen Standortvorteil für das Land begreifen[15], wurden nicht nur die gesetzlichen, sondern auch alle untergesetzlichen Vorschriften geschaffen[16], so dass mit der praktischen Anwendung der neuen Instrumente begonnen werden konnte. Beim Datenschutzaudit geht es darum, dass öffentliche Stellen – für Privatfirmen hat Schleswig-Holstein keine Gesetzgebungskompetenz – ihr Datenschutzkonzept freiwillig überprüfen lassen und gegebenenfalls ausdrücklich bestätigt bekommen, dass die Daten der Bür-

ger bei ihnen gesetzeskonform und sicher verarbeitet werden. Rechtsgrundlage sind § 43 Abs. 2 LDSG und die darauf fussenden Durchführungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz (ULD)[17]. Nachdem zunächst Pilotverfahren vorgeschaltet wurden, wurden 2002 die ersten „richtigen" Auditverfahren abgeschlossen. Sie basieren auf einer vertraglichen Vereinbarung zwischen dem ULD und der jeweiligen Behörde. Das Verfahren selbst vollzieht sich in den Stufen Bestandesaufnahme, Festlegung der Datenschutzziele, Einrichtung eines Datenschutzmanagements, Begutachtung durch das ULD und Verleihung des Auditzeichens. Kernbestandteil sind die Datenschutzziele, die eine Verbesserung des Datenschutzes im Auge haben und das Datenschutzmanagementsystem, das für ein dauerhaft gutes Datenschutzniveau sorgen soll. Wenn man aus den bisherigen Erfahrungen erste Schlüsse ziehen will, dann fällt auf, dass sich vor allem moderne Verwaltungsmanager für das Audit interessieren, also eine Klientel, die um das Thema Datenschutz sonst lieber einen weiten Bogen macht. Sie sind ehrgeizig und wollen „überall" gut sein, also auch beim Datenschutz. Weiterhin zeigt sich, dass überwiegend einzelne Verwaltungsverfahren auditiert werden, nicht die gesamte Datenverarbeitung einer Behörde. Die Vorschriften sehen dies mit gutem Grund vor, damit man sich dem Thema Audit vorsichtig und mit überschaubarem Risiko nähern kann. Alles in allem ist bemerkenswert, dass es ein ganz anderer Diskussionsstil ist, wenn jemand freiwillig und kooperativ auf das Thema Datenschutz zugeht, weil er nicht Kritik und Beanstandung fürchten muss, sondern sich sogar einen Vorteil verspricht. Wie formulierte ein Bürgermeister in Schleswig-Holstein kürzlich so trefflich: „So macht der Datenschutz Spass"!

Gütesiegelverfahren

Bei den Gütesiegeln für IT-Produkte steht die auch in anderen Datenschutzgesetzen anzutreffende[18] Bestimmung von § 4 Abs. 2 LDSG am Ausgangspunkt, wonach die Behörden vornehmlich solche Produkte einsetzen müssen, die mit den Bestimmungen von Datenschutz und Datensicherheit vereinbar sind. Solche Vorschriften bleiben solange ein frommer Wunsch, als derartige Produkte nicht für die Verwaltung gekennzeichnet sind. Deshalb hat Schleswig-Holstein sein Gütesiegelverfahren im Detail geregelt[19]. Es sieht im Kern eine „Arbeitsteilung" zwischen privaten Gutachtern und dem öffentlich-rechtlichen ULD vor[20]. Die Gutachter nehmen die eigentliche Begutachtung des Produkts vor und fertigen hierüber ein Gutachten an, das dem ULD vorgelegt wird. Das ULD prüft das Gutachten auf Schlüssigkeit und methodische Korrektheit und verleiht bejahendenfalls das Gütesiegel. Da den Gutachtern also eine wichtige Funktion zukommt, können nur solche Gutachter tätig werden, die beim ULD förmlich akkreditiert sind. Voraussetzung hierfür sind nach § 3 Abs. 1 der Gütesiegelverordnung die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit. Inzwischen sind elf Gutachter beim ULD akkreditiert, weitere Akkreditierungsverfahren sind anhängig. Die Kriterien, nach denen die Gutachter die Produkte begutachten und das ULD über die Vergabe des Gütesiegels entscheidet, ergeben sich aus § 2 Abs. 2 Nr. 4 der Gütesiegelverordnung. Danach müssen „besondere Eigenschaften des IT-Produkts, insbesondere zur Datenvermeidung und Datensparsamkeit (§ 4 Abs. 1 und § 11 Abs. 4 und 6 LDSG), Datensicherheit und Revisionsfähigkeit der Datenverarbeitung (§§ 5 und 6 LDSG), Gewährleistung der Rechte der Betroffenen (§§ 26 bis 30 LDSG)" vorliegen[21]. Dies alles ist jeweils im Hinblick auf den „Zweck und Einsatzbereich" (§ 2 Abs. 2 Nr. 3 Gütesiegel-VO) zu prüfen. Aus den für Zweck und Einsatzbereich geltenden rechtlichen Bestimmungen ist zunächst ein Anforderungsprofil zu entwickeln, an dem dann das Produkt zu messen ist. Das Gütesiegel selbst wird, wenn die Voraussetzungen vorliegen, vom ULD, also einer staatlichen Stelle, für die Dauer von zwei Jahren verliehen. Diese Tatsache sowie die dafür massgeblichen Gründe werden vom ULD veröffentlicht[22]. Das schleswig-holsteinische Gütesiegel ist keineswegs, wie man angesichts des gesetzgeberischen Ausgangspunktes annehmen könnte, auf die schleswig-holsteinische Verwaltung beschränkt. Voraussetzung für ein Gütesiegelverfahren ist nach § 1 Abs. 2 Gütesiegel-VO lediglich, dass das Produkt für den Einsatz in der Verwaltung geeignet ist. Weder muss es tatsächlich in der Verwaltung eingesetzt werden, noch muss auch nur die Absicht dazu bestehen. Das Produkt muss auch nicht in Deutschland, geschweige denn in Schleswig-Holstein hergestellt sein. Beispielsweise könnte ein

Schweizer Hersteller ein für die Verwaltung geeignetes Produkt, das er aber auf dem Privatmarkt in Asien anbieten will, zertifizieren lassen, wenn er sich davon einen Vorteil verspricht. Nach § 1 Abs. 3 S. 1 Gütesiegel-VO können zertifizierte Produkte „gekennzeichnet“ werden, was übersetzt in die Sprache der Marktwirtschaft heisst, dass damit im Rahmen der Wettbewerbsregeln nach Belieben Werbung gemacht werden kann. Viele Privatkunden werden vielleicht sagen, was gut für die Verwaltung ist, wird auch für mich nicht schlecht sein, und im Zweifel ein solches Produkt bevorzugen. Die Gütesiegel-VO möchte solche Wirkungen nicht verhindern. Im Gegenteil: Sie entspringt dem Grundgedanken, dass es nicht verwerflich ist, mit gutem Datenschutz auch gutes Geld zu verdienen. Das Motto „privacy sells“ in den Dienst der Grundrechtsverwirklichung zu stellen, ist der eigentliche Clou des marktwirtschaftlichen Datenschutzes[23]. Die bisherigen Erfahrungen des ULD lassen den Schluss zu, dass die marktwirtschaftliche, über Schleswig-Holstein hinauszielende, Botschaft des Gütesiegels made in Schleswig-Holstein ankommt. Die Mehrzahl der Gutachter kommt von ausserhalb Schleswig-Holsteins. Die Anfragen von Herstellern und die bei den Gutachtern anhängigen Gütesiegelverfahren weisen weit über den schleswig-holsteinischen Markt und auch über den öffentlichen Sektor hinaus. Bislang deutet alles darauf hin, dass das Kalkül von Landesregierung und Landesparlament, mit einem zukunftsweisenden Datenschutzkonzept den Standort Schleswig-Holstein im IT-Markt attraktiv zu gestalten, aufzugehen scheint.

Perspektiven

Wir haben gesehen, dass der Einstieg in marktwirtschaftliches Denken einen regelrechten Dominoeffekt auslösen kann, bei dem wir mit einem Grundrecht begonnen haben und über Marktvorteil, Datenschutzaudit und Gütesiegel am Ende bei so etwas wie Lifestyle gelandet sind. Wir sollten bei dieser schnellen Reise nichts verloren haben, schon gar nicht unser Grundrecht auf Datenschutz. Das brauchen wir in der entwickelten Informationsgesellschaft mehr denn je. Nicht nur jeder von uns als Individuum, sondern auch unser demokratisches Gemeinwesen, das ohne wirksamen Datenschutz in der Informationsgesellschaft nicht überleben kann. Marktwirtschaftlicher Datenschutz will und darf also nichts vom Grundrechtsschutz wegnehmen, sondern er soll die Realisierungschancen des Datenschutzes verbessern. Wir brauchen auch in Zukunft eine funktionierende, gut ausgestattete und zupackende Datenschutzkontrolle, denn nur mit schönen Worten und Gewinnerwartungen ist kein Datenschutz zu machen[24]. Marktwirtschaftlicher Datenschutz könnte aber auch die Datenschutzkontrolle verbessern. Wer mit Audit und Gütesiegel offensiv wirbt und den Kunden signalisiert, er wolle beim Datenschutz vorbildlich sein, der riskiert, dass das Publikum sein Augenmerk tatsächlich auf diesen Bereich lenkt. Tausende von aufmerksamen Kundenaugen sehen am Ende mehr als die wenigen staatlichen Datenschutzkontrolleure. Also: Nicht weniger, sondern unter dem Strich mehr Kontrolle wird die Folge sein. Der Staat tut gut daran, auch bei der Einführung von Audits und Gütesiegeln seine Hände im Spiel zu halten. Das Vertrauen des Publikums werden vornehmlich solche Gütesiegel bekommen, deren Vergabe der Staat als eine an der Marktkonkurrenz nicht beteiligte Instanz steuert. Am Idealsten ist es, wenn eine Datenschutzkontrollstelle, der die Bürger besonders vertrauen, beteiligt ist. In Schleswig-Holstein vermochte das Unabhängige Landeszentrum für Datenschutz die unterschiedlichen Aufgaben Kontrolle, Aufsicht, Beratung, Auditierung und Gütesiegelverfahren bislang gut miteinander zu kombinieren. Auf diesem Weg konnte sichergestellt werden, dass das Datenschutzgesetz einheitlich ausgelegt wird und Wirtschaft, Behörden, Bürgern und Kunden „Datenschutz aus einer Hand“ geboten werden konnte. Wenn man sich fragt, ob die Entwicklung von Audit und Gütesiegeln in einem einzigen Bundesland ideal ist, so muss man entschieden mit Nein antworten. Der IT-Markt ist international, deshalb müssten etwa auch die Standards für Datenschutzgütesiegel weltweit gelten. Da aber die Gesetzgebung in Deutschland schon auf Bundesebene nicht vorankommt, hat man sich in Schleswig-Holstein entschlossen, den Anfang zu wagen. Dass dabei eine singuläre Randlösung entwickelt wird, steht aus folgenden Gründen vermutlich nicht zu befürchten:

- Das Bundesinnenministerium hat dem Unabhängigen Landeszentrum für Datenschutz den Auftrag zur Erstellung eines Gutachtens erteilt,

in dem die in Schleswig-Holstein gemachten Erfahrungen für die kommende Bundesgesetzgebung nutzbar gemacht werden sollen.

■ Die Europäische Union fördert zwei Modellprojekte des ULD zum Thema Audit und Gütesiegel, die auch die Durchführung eines internationalen Kongresses am 25. August 2003 in Kiel vorsehen, bei dem die in Europa bestehenden Audit- und Gütesiegel-Vorhaben vorgestellt werden.

■ Im August 2001 wurde in Kiel die internationale Arbeitsgruppe PETTEP gegründet, die bis 2003 weltweite Standards für Datenschutz-Gütesiegel erarbeiten will[25]. Das ULD arbeitet bei PETTEP mit und kann so seine Erfahrungen einbringen. Der Datenschutz und insbesondere seine effektive Durchsetzung in der Praxis bleibt eine der zentralen Herausforderungen unserer Zeit. So kompliziert er im Detail erscheinen mag, im Kern geht es stets um einen fairen und korrekten Umgang mit personenbezogenen Daten. Die Methoden aber, mit denen dies erreicht werden kann, unterliegen angesichts der Dynamik der Informationstechnik einem raschen Wandel. Im Moment spricht vieles dafür, dass Audit und Gütesiegel in den kommenden Jahren für die Verwirklichung des Datenschutzes eine wachsende Bedeutung erhalten werden. Wer es gerne modisch mag, wird vielleicht Gefallen an der Formulierung finden: „privacy goes market".

Helmut Bäumler, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Hostein, Kiel

Nachdruck aus Digma 2003.1 mit Genehmigung des Autors

Endnoten

1 § 17 Mediendienstestaatsvertrag v. 1997, abgedruckt in Telekommunikations- und Multimediarecht, 3. Aufl., München 2001, 161.

2 Vgl. z. B. § 11c Brandenburgisches Datenschutzgesetz v. 21.12.1998, GVOBI S. 243, § 10a Datenschutzgesetz Nordrhein-Westfalen, GVOBl 2000, 242.

3 V. 18.5.2001, BGBl I, 904.

4 Gesetz v. 9.2.2000, GVOBl 20002, 169.

5 Gesetz v. 28.3.2002, GVOBl 2002, 154.

6 Landesverordnung über ein Datenschutzaudit v. 3.4.2001, GVOBl 2001, 51 (im Folgenden Text „Gütesiegelverordnung").

7 Vgl. dazu ausführlich HELMUT BÄUMLER / ALBERT V. MUTIUS (Hrsg.), Datenschutz als Wettbewerbsvorteil, Braunschweig/Wiesbaden 2002.

8 HORST. W. OPASCHOWSKI, Was will der Verbraucher?, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 13ff.

9 Vgl. statt vieler MARIT HANSEN, Privacy Enhancing Technologies in ALEXANDER ROSSNAGEL, Handbuch des Datenschutzrechts, München 2003, i.E., m.w.N.

10 Grundlegend JOHN BORKING, DuD 1996, 654.

11 Vgl. dazu auch EDDA MÜLLER, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 20ff., und THILO WEICHERT, a.a.O., 27ff.

12 Einzelheiten bei HELMUT BÄUMLER, DuD 2002, 325ff, vgl. zum marktwirtschaftlichen Datenschutz grundlegend auch ALFRED BÜLLESBACH, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 45ff.

13 ALBERT V. MUTIUS, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 81ff.

14 Grundlegend zum Datenschutzaudit ALEXANDER ROSSNAGEL, Datenchutzaudit, Braunschweig 2000 sowie ders. in HELMUT BÄUMLER, Der neue Datenschutz, Neuwied 1998, 65ff.

15 So der Titel des Beitrags von HEIDE SIMONIS, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 225ff.

16 Abrufbar unter http://www.datenschutzentrum.de/audit und http://www.datenschutzzentrum.de/guetesiegel

17 Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG v. 22.3.2001, Amtsbl. S-H 13/2001, 196; zum schleswig-holsteinischen Datenschutzaudit vgl. grundlegend CLAUDIA GOLEMBIEWSKI (Fn. 7), 107ff.

18 Vgl. z.B. § 5 Abs. 4 Hamburgisches Datenschutzgesetz v. 30.1.2001, HmbGVBl 9.

19 Landesverordnung über ein Datenschutzaudit v. 3.4.2001, GVOBl, 51.

20 Zum Verfahren im Einzelnen vgl. ausführlich ANJA DIEK, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 7, 157ff.

21 Einzelheiten zu den Kriterien bei MARIT HANSEN / THOMAS PROBST, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 163ff.

22 http://www.datenschutzzentrum.de/guetesiegel. Bei der Abfassung dieses Textes hatten bereits die ersten Gütesiegelverfahren begonnen. Angesichts der Dynamik, die im IT-Sektor und speziell auch im Bereich des Datenschutzaudits herrscht, ist zu erwarten, dass die Entwicklung beim Erscheinen des Beitrages schon wieder ein Stück weiter ist.

23 HELMUT BÄUMLER, DuD 2002, 325 ff.

24 Hierin ist BEAT RUDIN, „Privacy" nicht privatisieren!, in: digma 2002.1, 52, zuzustimmen.

25 Einzelheiten bei MARIT HANSEN / THOMAS PROBST, in: HELMUT BÄUMLER / ALBERT V. MUTIUS (Fn. 7), 7, 163 (178f).

Datenschutz

Die Modernisierung des Datenschutzes und die Rolle des eidgenössischen Datenschutzbeauftragten

Deutsche Übersetzung des Artikels aus *NewsLetter* 1/03.

Der deutsche Gesetzgeber entdeckt zunehmend Datenschutzaudit und Gütesiegel. Beides ist notwendig, wenn der Datenschutz eine marktwirtschaftliche Komponente erhalten und künftig stärker von der Informationstechnik unterstützt werden soll. Da im Bund und in den anderen Ländern noch Ausführungsgesetze notwendig sind, gibt es bislang nur im Bundesland Schleswig-Holstein praktische Erfahrungen. Sie sind durchgängig gut, denn Audit und Gütesiegel erschliessen dem Datenschutz neue Gesprächspartner, geben der Prävention mehr Chancen und belohnen diejenigen, die das Datenschutzrecht gut umsetzen. Firmen und Behörden machen die angenehme Erfahrung, dass man mit Datenschutz auch etwas gewinnen, nicht nur verlieren kann.

Einführung

Das Bundesgesetz über den Datenschutz ist zehn Jahre alt. Diesen Zeitpunkt hat der Bundesrat gewählt, um eine Teilrevision des DSG durchzuführen. Anfang 2003 wird er dem Parlament die diesbezügliche Botschaft unterbreiten. Die Revision greift zwei parlamentarische Motionen auf, welche einen erhöhten Datenschutz im Bereich der Online-Verbindungen und erhöhte Transparenz bei der Erhebung von Personendaten anstreben. Ausserdem soll diese Revision der Schweiz erlauben, das Zusatzprotokoll zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren. Dieses Protokoll betrifft die Aufsichtsbehörden und die grenzüberschreitenden Datenflüsse. Die Revision ermöglicht zwar eine Annäherung an das Europarecht und an die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, stellt aber keine Umsetzung dieser Richtlinie dar. Wenn die bilateralen Verhandlungen II zwischen der Schweiz und der Europäischen Union zum Abschluss kommen, wird eine substantiellere Revision des Gesetzes erforderlich sein, um unser Recht mit den europäischen Auflagen vollkommen zu harmonisieren, da die Richtlinie zum gemeinschaftlichen Besitzstand (acquis communautaire) gehört, den die Schweiz dann übernehmen müsste.

Revision des Bundesgesetzes über den Datenschutz

Der Revisionsentwurf stärkt die Position der betroffenen Personen, insbesondere mit der Einführung der Transparenzpflicht beim Beschaffen von Personendaten. Jedes Beschaffen von Daten muss in der Zukunft für die betroffene Person erkennbar sein und Gegenstand einer aktiven Information durch die Bearbeitungsverantwortlichen bilden, falls es sich um besonders schützenswerte Daten oder Persönlichkeitsprofile handelt. Im privaten Sektor wird das Recht, eine Bearbeitung zu verweigern, wirksamer gestaltet, indem der Bearbeitungsverantwortliche aufgefordert wird, zu den Gesuchen von Einzelpersonen Stellung zu nehmen. Die grenzüberschreitenden Datenflüsse sollen überarbeitet werden. Zum einen wird das System der vorhergehenden Meldung aufgehoben; zum anderen wird das Verbot der Übermittlung zwar beibehalten, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein dem schweizerischen gleichwertiger Datenschutz fehlt, aber das Gesetz sieht Ausnahmeregelungen vom Verbot vor (Rückgriff auf vertragliche Datenschutzklauseln, Datenschutzreglement für Unternehmensgruppen). Die Meldepflicht für Datensammlungen wird für Bundesstellen wie für Privatpersonen beibehalten. Allerdings sollen Ausnahmen von der Meldepflicht in das Gesetz eingeführt und das Meldeverfahren vereinfacht werden: In absehbarer Zukunft wird der Inhaber einer Datensammlung die Möglichkeit erhalten, seine Register online anzumelden.

Ausserdem ist in Anlehnung an das Umweltgesetz und an das deutsche Datenschutzrecht geplant, die Zertifizierung der Produkte und der Personendatenbearbeitungssysteme zu fördern (Audit, Datenschutz-Qualitätslabel).

Zertifizierungsverfahren (Audit)

Die Zertifizierung des Datenschutzes bildet für den Bearbeitungsverantwortlichen einen Anreiz, freiwillig ein Verfahren einzusetzen, das zur konstanten Verbesserung des Datenschutzes beitragen soll. Für Unternehmen bzw. staatliche Stellen, die sich dem Verfahren unterziehen, ist auch ein Vorteil verbunden, weil ihnen nämlich ein Image der Übereinstimmung mit den Datenschutzauflagen vermittelt wird. In einer globalisierten Welt, in welcher der Informationsaustausch immer alltäglicher wird, spielt der Datenschutz eine unverzichtbare Rolle und erweist sich insbesondere mit Blick auf den E-Commerce oder die Online-Administration als Vertrauens- und Akzeptanzfaktor. Insofern entwickelt sich ein wirksamer Datenschutz auch zu einem Wettbewerbsfaktor.

Das Datenschutzaudit erlaubt die Stärkung der Verantwortung der Einzelperson und die Ankurbelung des Wettbewerbs. Ausserdem wird die kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit vorangetrieben und ein ständiges Lernsystem begründet. Die Zertifizierung und die Erteilung eines Qualitätslabels „Datenschutz“ implizieren, dass die gesetzlichen Datenschutzauflagen bei der Entwicklung von Datenbearbeitungssystemen in technischer und organisatorischer Hinsicht berücksichtigt wurden, d.h. dass diese Auflagen mit Hilfe von technischen Normen erfüllt werden. Die Effizienz des Qualitätslabels beruht auf der Einhaltung verschiedener Kriterien, insbesondere:

- das Zertifizierungsverfahren und der Prozess der Label-Erteilung müssen transparent sein und auf international anerkannten Kriterien beruhen;
- die Auswertungskriterien sollen klar definiert und nach Normen festgelegt sein, die den Gesetzesauflagen entsprechen;
- der Label muss von einer im Rahmen eines Audit-Verfahrens zugelassenen und qualifizierten Einrichtung erteilt werden.

Vor der Erteilung eines Datenschutz-Qualitätslabels ist im Rahmen des Audit-Verfahrens sicherzustellen, dass die Bearbeitung der Personendaten im Einklang mit den Gesetzesauflagen erfolgt. Der Eidgenössische Datenschutzbeauftragte (EDSB) definiert in seinem achten Tätigkeitsbericht folgende Auflagen, die zu überprüfen sind:

- Transparente Information an den Benutzer/Kunden (z.B. Privacy Policy).
- Erfüllung der gesetzlichen Anforderungen bei Datenbearbeitungen (wie Kriterien zur Speicherung, Löschung und Weitergabe von Personendaten).
- Gewährung von Auskunfts- und Berichtigungsrecht sowie Klagerechte bei Streitfällen oder Persönlichkeitsverletzungen.
- Gewährung eines Wahlrechts an die Benutzer/Kunden für die Verwendung seiner Daten.
- Gewährung der Datensicherheit durch technisch-organisatorische Massnahmen.

Die Erteilung eines Datenschutz-Qualitätslabels stellt keineswegs eine endgültige Errungenschaft dar. Es ist notwendig, weitere regelmässige (interne und externe) Kontrollen durchzuführen. Diese Kontrollen müssen auf einem verlässlichen Prozess beruhen und von unabhängigen, im Kontrollbereich kompetenten Stellen durchgeführt werden. Wenn die Bestimmungen und Gesetzesauflagen des Datenschutzes verletzt werden, sind Massnahmen und Sanktionen zu ergreifen, die bis zum Rückzug des Qualitätslabels reichen können.

Grundsätzlich bleiben die Zertifizierung und die Erteilung von Qualitätslabels die Aufgabe der privaten Unternehmen. Der Gesetzgeber erlässt lediglich Vorschriften zur Anerkennung der Zertifizierungsverfahren und zur Einführung der Labels. Es wäre denkbar, die Zertifizierungsstellen einer Akkreditierungspflicht zu unterstellen und für die erteilten Labels zu werben. Der Gesetzgeber müsste dabei das internationale Recht sowie die international anerkannten technischen Normen berücksichtigen. Der ESDB sollte keine Stelle für die Zertifizierung bzw. Label-Erteilung sein. Dagegen sollte er die bei der Zertifizierung eingesetzten Methoden prüfen und gegebenenfalls Empfehlungen abgeben können (Datenschutzrevision). Im Rahmen seiner Befugnisse sollte der EDSB bei Bedarf nicht nur sicherstellen, dass die zertifizierten Unternehmen die Datenschutzauflagen einhalten, sondern

auch, dass die Prüfstellen gemäss den Anforderungen des Datenschutzes arbeiten.

Die Zertifizierung und die Erteilung von Datenschutz-Qualitätslabels bilden eine Anreizmassnahme für die Eigenverantwortung der Unternehmen, die Daten bearbeiten. Weitere Massnahmen, so z.B. der Anreiz für die Verwendung datenschutzfreundlicher Technologien und die Verabschiedung sektorieller Verhaltenskodizes, könnten in Betracht kommen.

Die Befugnisse des EDSB

Die Datenschutzbehörden, insbesondere der EDSB, bemühen sich in ihrem Vorgehen, die betroffenen Personen und die Bearbeitungsverantwortlichen für die mit der Bearbeitung von Personendaten verbundenen Risiken zu sensibilisieren. Das beinhaltet insbesondere eine aktive Informationspolitik, eine Risikoevaluation, die Ausarbeitung von „Werkzeugen“ (in Absprache mit den betroffenen Kreisen), um die Datenschutzauflagen zu verwirklichen und die Gefahr einer Beeinträchtigung der Rechte der betroffenen Personen zu verringern, sowie die Kontrolle der Gesetzesanforderungen.

Die Wirksamkeit des Datenschutzes hängt auch von der Rolle und den Zuständigkeiten von Aufsichtsbehörden wie dem EDSB ab. Die höhere Verantwortung für Inhaber von Datensammlungen muss so die Einführung von präventiven und (im Missbrauchsfall) repressiven Kontrollmitteln nach sich ziehen. In Zukunft müssten demnach die Aufsichtsbehörden eine pro-aktivere Rolle spielen. Ziel der Datenschutzbehörden ist es, zu vermeiden, dass Einzelpersonen bei der Bearbeitung von Personendaten über sie völlig schutzlos sind, aber nicht, die Datenbearbeitung an sich zu verhindern. Daher muss eine Politik entwickelt werden, welche die Anerkennung und die Achtung der Datenschutzgrundsätze fördert und den betroffenen Personen die wirksame Ausübung ihrer Rechte erlaubt. Die Aufsichtsbehörden haben folglich die Aufgabe, zu überprüfen, dass diese Regeln befolgt und in die Datenverarbeitungsabläufe sowie in die Informationssysteme integriert werden, indem sie insbesondere den Einsatz von Technologien zur Integration der grundlegenden Prinzipien des Datenschutzes vorantreiben.

Der EDSB muss dagegen die Achtung der Gesetzesauflagen nicht nur kontrollieren. Bei Verletzung dieser Auflagen soll er auch die angemessenen Massnahmen ergreifen und gegebenenfalls Sanktionen verhängen können. Die Effizienz der Aufsicht setzt (heute unzureichende) Ressourcen und Entscheidungsbefugnisse voraus. Ähnlich wie andere Datenschutzbehörden in Europa und sonstige Aufsichtsbehörden in der Schweiz, z.B. die Eidgenössische Wettbewerbskommission, sollte auch der EDSB ermächtigt werden, Sanktionen zu verhängen.

Jean-Philippe Walter, Dr. iur., Stellvertreter des Eidgenössischen Datenschutzbeauftragten

Express Line

A Word from the Chair

A review of chapter web sites has been completed by the Membership Board to determine the winners of the 2002 Web Site Award. Those sites awarded a "gold" rating will receive the honor of placing an ISACA award notation on their home page. Chapters that attained the gold rating for their web sites (85 or higher out of 100 possible points) include Denmark, Germany, Hong Kong, London, Los Angeles, Montevideo, New Jersey, Puget Sound, Quebec, Raleigh and Tampa. We commend these chapters for their excellence in the design, content and management of their chapter web sites. The award criteria are posted on the awards page of the chapter leadership area on the ISACA web site.

Howard Nicholson
Chair, Membership Board

2003 Annual General Meeting

ISACA will hold its 2003 Annual General Meeting on Monday, 21 July 2003, in Los Angeles, California, USA.

Included on the agenda will be the president's annual report, the treasurer's report, ratification of significant board actions from the 2002-2003 administrative year and an inaugural speech from the newly inducted International President.

All ISACA members are invited to attend.

Certification Update

CISA Appeals to a Variety of IT Professionals

A profile of the nearly 20,000 CISAs who are actively certified indicates the important role, managerial influence and authority that CISAs wield. CISAs are today's and tomorrow's leaders. They are recognized for their technical and business knowledge and their ability to identify, evaluate and recommend solutions to mitigate IT system vulnerabilities.

Currently, 3,000 CISAs serve in executive positions:

- 400 CISAs are the chief executive officer (CEO) or chief financial officer (CFO) at their organization
- 700 CISAs serve as the chief information officer (CIO) or IS security director
- 1,900 CISAs are the audit director or audit partner at their organization or firm

Presently, 4,300 CISAs serve in managerial positions:

- 2,500 CISAs serve as IS audit managers
- 1,800 CISAs serve as IS or IS security managers

Currently, 9,800 CISAs serve in a practitioner position

- 6,500 serve as an IS auditor
- 3,000 are employed as IS security staff or consultants
- 300 are employed as IS vendors, suppliers and educators

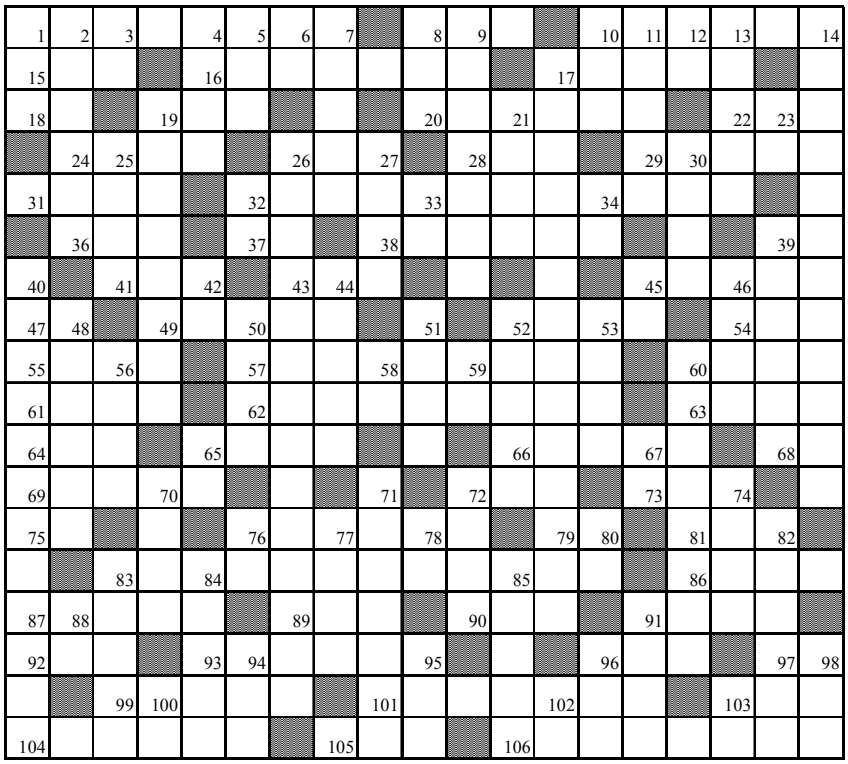
In addition, 2,500 others are CISA certified, but have not recently reported their job responsibilities.

Research Projects in Progress with Target Release Dates

- Biometrics project-third quarter 2003
- COBIT mapping project-third quarter 2003
- Identity management project-third quarter 2003
- Oracle database project-third quarter 2003
- OS/390 (Z/OS) project-fourth quarter 2003
- Wireless communication project-fourth quarter 2003
- Security and Risk Management in an Oracle Financial Environment-fourth quarter 2003
- Security and Risk Management in a PeopleSoft Environment-fourth quarter 2003
- Enterprise information integrity project-fourth quarter 2003

The ISACA Crossword Puzzle 3/03

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



Waagrecht: **1 Schicksalsschlag**; 8 Chef im Kloster; 10 Schriftart; 15 Sinnesorgan; 16 erteilt Ratschläge; 17 grosser Wasserbehälter; 18 intl Zeichen für Südost; 19 plastikartiges Material; 20 Dauerwurstart; 22 nordischer Wurfspeer; 24 Edelgas; 26 „Verlustposten" einer Schweizer Fluggesellschaft; 28 tief (frz); 29 Wetterlage im Genitiv; 31 Dung; **32 nicht nur für ein Rechenzentrum unangenehm;** 36 Feldmass (schweizerisch); 37 japanisches Brettspiel; 38 Schnitterwerkzeug (Mz); 39 kurzer Sportclub; 41 Seele (frz); 43 most loved element (Abk); 45 Lurch; 47 babylonischer Erdgott; 49 Planskizze; 52 Indianerausruf; 54 Lebensgemeinschaft; 55 Stieleke's Vorname; **57 zuviel Regen oder 1 waagrecht können die Ursache sein;** 60 Modeschöpfer; 61 Tatkraft; 62 Verbrechen; 63 Herzstück von jedem Museum; 64 Nordlandtier; 65 ohne Inhalt; 66 störendes Geräusch; 68 Anschrift für Unbekannt; 69 Stenographiezeichen; 72 schnelle Messeinheit (Abk); 73 in der italienischen Liebeserklärung nicht wegzudenken; 75 AZ der ehemaligen deutschen Hauptstadt; 76 Dummheit; 79 frz Adelsprädikat; 81 hat (engl); 83 ernst nehmen; 86 Balte; 87 Fabrik (frz); 89 Stimmlage; 90 mittelhochdeutsche Verkleinerungssilbe; 91 da; 92 ausschliesslich; 93 Bodenbelag; 96 Grundfarbe; 97 Staatengemeinschaft (Abk); 99 Krankheit; 101 Dachboden; 103 Wachholderschnaps; 104 Trinkgefäss (Mz); 105 für (lat); 106 Sehenswertes (Mz).

Senkrecht: 1 Göttin der Morgenröte; 2 griechische Göttin; 3 akademischer Kurztitel; 4 flach; 5 wetten (engl); 6 persönliches Fürwort; 7 Gegenpunkt des Zenith; 8 Aufforderung an das Reh, sich gütlich zu tun; 9 belgische Region; 10 Form von kommen; 11 afrikanische Befreiungsbewegung; 12 registered nurse (Abk); 13 Windfang; **14 vermindert das Risiko; 17 oft Folge der Bekämpfung von 40 senkrecht (Mz);** 19 russischer Bluffer; 21 Parasit; 23 Ehrenfahne (Abk); 25 biblischer Tempelbauer; **26 wohl der GAU an sich;** 27 Blume; 30 Wallenstein's Feldherr; 32 AZ aus der Ostschweiz; 33 frz rückbez Personalpronomen; 34 tonloser Anhänger; 39 lieblich; **40 Katastrophenursache;** 42 pers Fürwort; 44 Augendeckel (Mz); 45 Motorwerkstatt (Abk); 46 poetisch kaum hörbar; 48 ohne Begleitung; 50 schmucklos; 51 Kunstgöttin; 52 biblische Hymne; 53 Schusterwerkzeug; 56 Dimensionsbegriff; 58 CZ Rubidium; 59 zwei gleiche Konsonanten; **60 Grund vieler Katastrophen;** 65 span Buchstabe; 67 ägyptischer Sonnengott; 70 nordischer Hirsch; 71 verführerischer Tand; 72 Fluss vom Drusberg nach Zürich; 74 Wüsteninsel; 76 Einheitspreis (Abk); 77 Armknochen; 78 der Vorfahre von 97 waagrecht (engl); 80 verliert bei Martina diesen Namen, den er seit dem Maloja trug; **82 Arbeits-**

niederlegung; 83 Krankheitserreger; 84 Küchengerät; 85 Papstkrone; 88 ehemaliges AZ aus Moskau und Umgebung; 91 inhaltlos; 94 persische Rohrflöte; 95 transaction sequence option; 96 Ruderclub Birsfelden (Abk); 98 frz unbest Artikel; 100 pers Fürwort; 102 en vogue; 103 Zürcher Sportclub.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, 8135 Langnau a/A. Lösungen werden auch entgegengenommen unter der e-mail-Adresse mbretscher@kpmg.com.
Einsendeschluss ist der 29. August 2003.

Das Minimum von fünf Lösungen wurde diesmal bis zum Redaktionsschluss nicht erreicht. Damit verfallen die als Preis ausgesetzten US$ 50 in den (nächsten) Jackpot. Dagegen hat Marina Müller den bisherigen Watson-Jackpot (US$ 150) gesprengt! Herzliche Gratulation. Ihr ist nämlich aufgefallen, dass das Kreuzworträtsel in deutscher Sprache verfasst ist, das Lösungswort dagegen in englischer Sprache auftritt. Und genau dies war die gesuchte Unstimmigkeit. Keep looking for the oddities, Watson!

Hier nochmals die Regeln des ISACA Crossword Puzzles:
Lösungswort: Für jedes Rätsel setzt das Switzerland Chapter einen Preis von US$ 50 aus. Gewinner(in) ist die/der Einsender/in des richtigen Lösungswortes, falls mindestens fünf Einsendungen bis zum Redaktionsschluss eintreffen. Liegen mehrere richtige Lösungen vor, entscheidet das Los anlässlich der Redaktionssitzung. Treffen bis Redaktionsschluss weniger als fünf Antworten ein, verfallen die ausgesetzten US$ 50 in den Watson-Jackpot.
Watson: In jedem Kreuzworträtsel ist eine kleine Unstimmigkeit versteckt. Wer diese herausfindet, leert den Watson-Jackpot unabhängig davon, wie viele Einsendungen eintrafen und unabhängig davon, wer allenfalls den Lösungswort-Preis erhielt. Ist der Watson-Jackpot leer, füllt ihn der Redaktor mit US$ 50 auf.
Alle Preise werden nicht in bar, sondern in Form von Gutschrift auf Bezüge im *ISACA Bookstore*, ausbezahlt.
Die Entscheide der Redaktionskommission sind nicht anfechtbar.

Lösung Crossword Puzzle 2/03:
Translucent

Versteckte Einzelheit: Das Kreuzworträtsel ist deutsch, das Lösungswort englisch!

Waagrecht: 1 ajour; 5 Besan; 9 anonym; 14 Sud; 15 Sprutz; 17 Uri; 18 UNO; 19 TW; 20 Kroete; 21 Embleme; 23 (Three Faces of) Eve; 25 Eger; 27 RSRM; 29 Bleirohr; 31 gare; 33 neve; 34 R(e)née; 35 Pfote; 37 har; 38 Scheisser; 41 (R)oggen; 42 NW; 43 Toess; 44 es; 46 Lil; 48 EDI; 49 *Schluessel*; 54 Oes(terreich); 56 Hel; 57 *zweideutig*; 58 ELC; 59 Tee; 61 el; 62 rasch; 64 NN; 65 Bulle; 67 Ehrfurcht; 70 leg; 71 Elena; 73 Leth(e); 74 Erin; 75 Snob; 76 Brenners; 78 Mesa; 80 Gote; 82 âne; 83 Sonette; 85 arisch; 88 GE; 90 Ion; 91 Tag; 92 Kresse; 93 Dee; 94 queren; 95 Unart; 96 Rolle.

Senkrecht: 1 Ast; 2 Juwel; 3 Od; 4 R(a)s(e)r; 5 Bré; 6 Euterpe; 7 Steg; 8 AZ; 9 arbre; 10 Nils; 11 *Nummer*; 12 YNE; 13 MO; 16 poroes; 17 um; 20 keines; 21 Erato; 22 Ernani; 24 verheilt; 26 ego; 28 *Verwischtes*; 29 Bestehendes; 30 Reisszeug; 32 *Register*; 36 Freude; 37 hellgruen; 39 *Code*; 40 Schellen; 45 Seelen; 47 *loeschen*; 50 CW; 51 Li; 52 su; 53 Ei; 55 Elch; 60 Ebenen; 63 artnah; 66 Eloge; 68 Haberer; 69 Fleiss; 70 Limone; 72 EBO; 77 *Regel*; 79 Sète; 81 Tara; 83 sou; 84 TG; 86 Ist; 86 Cer; 89 eee; 90 IQ; 92 KN; 93 DL.

DACH-News

D: Aktivitäten des German Chapter

Kurz vor den Sommerferien stellt sich noch einmal die Frage, was im Germany Chapter in den letzten zwei Monaten eigentlich so passiert ist.

Das herausragende Ereignis war natürlich die Vorbereitung auf das diesjährige CISA-Examen, das am 14. Juni 2003 zusammen mit dem erstmalig zur Austragung gelangenden CISM-Examen stattfand.

Die beiden in Hamburg und Frankfurt angebotenen CISA-Vorbereitungskurse stießen auf sehr großes Interesse bei den CISA-Kandidaten. Insgesamt haben mehr als 50 Kandidaten an den beiden Kursen sowie knapp 30 am CISA-Testexamen in Frankfurt teilgenommen. Die im vergangenen Jahr erprobte Form des Vorbereitungskurses als zweimaliges Wochenendseminar hat sich auch dieses Jahr wieder bewährt und führt hoffentlich wie in den Vorjahren zu einer höheren Erfolgsquote der Deutschen CISA-Kandidaten im Vergleich zum internationalen Durchschnitt.

Zum Schluss möchten wir noch alle Mitglieder dazu auffordern, den *NewsLetter* verstärkt als Basis für den Wissens- und Erfahrungsaustausch zu nutzen. Hierzu freuen wir uns natürlich besonders über Artikel aus der Praxis, wissenschaftliche Themen oder Berichten über Seminare (Ansprechpartner bei Fragen: Ingo Struckmeyer).

Auch ermuntern wir alle Mitglieder, sich in bereits bestehenden Arbeitsgruppen (wie LINUX) zu engagieren oder gern auch neue Arbeitsgruppen in den Regionen ins Leben zu rufen, da der Berufsverband letztlich von den Aktivitäten seiner Mitglieder lebt. Hierzu kann jede(r) Kontakt mit einem unserer Vorstandsmitglieder aufnehmen, um gemeinsam eine Arbeitsgruppe aufzusetzen. Informationen zu bestehenden Arbeitsgruppen sind auf der Homepage des Germany Chapters (www.isaca.de) zu finden.

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: 21.–24. März 2004.

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

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 Einführung von IT Governance

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

Die ehemalige IG Anwendung von COBIT wird mit einer angepassten Zielsetzung reaktiviert.

Kick-off-Sitzung: Aufgrund des verspäteten *NewsLetter*-Versandes konnte der Anmeldetermin nicht eingehalten Werden. Wir werden die Kick-off-Sitzung im nächsten *News-Letter* neu ausschreiben.

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 Outsourcing/ Insourcing

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

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

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

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

IG MIS/EIS/DWH

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

Letzte Sitzung: Die letzte Sitzung fand am 6. Juni 2003 bei Ernst & Young in Zürich statt. Folgende Themen wurden besprochen:

- Referenzmodell Data Load: Das Referenzmodell wurde von H. Stauffer nochmals kurz überarbeitet. Für das weitere Vorgehen siehe unter Risk Matrix.
- Risk Matrix: Sie wurde von M. Maes und H. Stauffer reviewed. Die Matrix wurde nun bis zum Schritt Reporting als erstes Ergebnis der IG MIS/EIS verabschiedet.
- Publikation Ergebnisse: Die Risk Matrix soll zusammen mit dem Data Load Modell, dem Glossar und der Literaturliste nach einem Review durch ISACA CH auf deren Homepage öffentlich zugänglich gemacht werden.
- Weiteres Vorgehen: Die IG ist der Auffassung, dass sich ein DWH-Projekt von einem normalen Projekt unter diversen Aspekten unterscheidet. Deshalb soll für folgende Themen ein Fact Sheet mit den wesentlichen Punkten (Problemstellung und Prüfungsansätze) von den einzelnen Mitgliedern der IG erstellt werden. Diese Themen werden dann von der IG MIS/EIS bearbeitet:
- Projekt Management und Projekt Abwicklung
- Datenschutz und sonstige Regulatoren
- Change and Configuration Management
- Berechtigungen
- Disaster Recovery Planning

Nächste Sitzung: Mi, 15. Oktober 2003, 09:15 bei E&Y Zürich, Bleicherweg 5. Stock
Für Informationen wenden Sie sich bitte an Daniel Oser. Weitere Mitglieder sind stets herzlich willkommen!

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 Tipps (alle)

Die für 21. Mai 2003 geplante Sitzung ist ausgefallen und wird auf 13. November 2003 verschoben.

Nächste Sitzungen: Donnerstag, 13. November 2003. Ort wird noch bekannt gegeben
Voraussichtliche Themen:

- Enterprise oder die neue Architektur der SAP
- Berechtigungskonzept BV
- Java und ABAP
- Erfahrungen und News

Der katastrophale Limerick

Eine Revisorin wurde geschickt zu prüfen die Bücher des Scheichs von Qatar
Als sie ihn sah, rief sie entsetzt: "Der schaut aus wie mein eigener Vatta!"
Sie konsultierte und befragte all seine Gofen,
Die sangen ihr die Mär in mehreren Strophen,
Die letzte war über die Mutter des Mädchens, und die war nun wirklich die Kata-.

A criminal hacker was pestering CISAs with spamming,
His actions caused thousands of mail boxes jamming,
A cute little gals' files looked catastrophic,
But she took it in a way rather philosophic;
Because she relied on her disaster recovery planning.

Veranstaltungen

e-biz Security Lab	8.–10. Juli 2003 Rapperswil, 3 Tage, ISACA
The Audit College	11.–15. August London, 5 Tage, MIS
SAP R/3 für Wirtschafts- und Informatikprüfer	12.–15. August 2003 Stuttgart, 4 Tage, ISACA
Internet Security Lab	20.–22. August 2003 Zürich, 3 Tage, ISACA
Informationssicherheit im Gesundheitsbereich	27. August 2003 Zürich, 16.30–17.30, ISACA
Application Security Lab	27.–29. August 2003 Zürich, 3 Tage ISACA
IT Security Awareness von A bis Z	24. September 2003 Zürich, 16.30–17.30, ISACA
Wireless Network Security and Audit	September 2003 London, MIS
Cryptography, Fundamentals and Applications	6.–9. Oktober 2003 Advanced Technology Seminars, 4 Tage, Engelberg
Securing and Controlling Oracle Databases	13.–14. Oktober 2003 London, 2 Tage, MIS
Audit and Security of Oracle Financials and More	15.–17. Oktober 2003 London, 3 Tage, MIS
IT Performance Measurement	29. Oktober 2003 Zürich, 16.30–17.30, ISACA
Internet Security Lab	5.–7. November 2003 Zürich, 3 Tage, ISACA
Application Security Lab	12.–14. November 2003 Zürich, 3 Tage, ISACA
Network Security Conference	17.–19. November 2003 Mailand, 3 Tage, ISACA
Federated Identity Management	26. November 2003 Zürich, 16.30–17.30, ISACA

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
Markus Gaulke
Marie-Curie-Str. 30
D-60439 Frankfurt
Tel. +49 (69) 9587-2313
MarkusGaulke@kpmg.com

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

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

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

Publikationen
Ingo Struckmeyer
comdirect 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 43 285 69 36
Fax. +41 43 285 33 69
daniela_gschwend@swissre.com

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

Kassier
Pierre A. Ecoeur, CISA
Thurgauer Kantonalbank
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/CISM-Koordinator
Thomas Bucher
Ernst & Young AG
Postfach
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 40 14
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
admin@isaca.ch
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
Rigistrasse 3
CH-8703 Erlenbach
Tel. +41 1 910 96 33
Handy: +41 79 776 09 82
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch