Nr. 79 | April 2006

Schwerpunkt-Thema:

IT-deliktische Handlungen

Inhaltsverzeichnis

Editorial 4

IT-deliktische Handlungen – Wirtschaftskriminalität in der Schweiz 5

IT-deliktische Handlungen – Computerforensik und Kriminalität 7

IT-deliktische Handlungen – Prüfungsstandard 240 10

Sécurité TEI – Éléments critiques pour la réussite d'un programme de sécurité des informations 12

The ISACA Crossword Puzzle 14

Express Line 16

DACH-News 17

Veranstaltungen 24

Vereinsadressen 26

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis International
WSJ 210.12.31
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich
mbretscher@kpmg.com

Satz und Gestaltung:
Steag & Partner AG
Francesca Lüscher Baglioni,
9000 St. Gallen

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.

Preise:
Mitglieder gratis
Abonnement CHF 35.–/Jahr
Einzelnummer CHF 10.–

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

Erscheint 5 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Thema: CobiT 4.0): Juli 2006, Redaktionsschluss: 23. Juni 2006

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Editorial

Deliktische Handlungen – Verantwortung des Abschlussprüfers

Wer ist dafür verantwortlich, dass das Geschäft orgnungsgemäss geführt wird und dass deliktische Handlungen aufgedeckt – oder besser verhindert – werden? Spontan würden wir antworten: Die Geschäftleitung schlussendlich.

Das dürfte wohl stimmen, mit der Anmerkung: Nicht nur! Welche Verantwortung trifft den Abschlussprüfer, deliktische Handlungen aufzuspüren?

Was sind eigentlich deliktische Handlungen? Welche Aktivitäten sind strafrechtlich relevant, gehören „Fehler“ auch in diese Kategorie? Der Fall SAirGroup beschäftigt derzeit das Bezirksgericht Bülach mit genau solchen Fragen: Führungsverantwortung und strafrechtliche Relevanz von Entscheiden.

Wo wir schon beim Management sind, auf welcher Etage werden am meisten deliktische Handlungen vorgenommen?

Doch zurück zu den Abschlussprüfern. Sind sie nun verantwortlich für das Aufdecken von Unrechtmässigkeiten, bzw. mehr brisant ist die Gegenfrage: Sind Abschlussprüfer haftbar für das Nicht-Aufdecken ebensolcher Unrechtmässigkeiten? Die Fälle Enron und Co. sowie deren Folgen für die Berater- und Prüferbranche sind Ihnen bestimmt noch in bester Erinnerung.

Ebenso schwerwiegend war der Einfluss auf neue Gesetzgebungen (SOX hält auch in der Schweiz Einzug, wenn auch nicht in genau der gleichen Form). In Anbetracht dieser (kürzlichen) Fälle: Wurde in den vergangenen Jahren mehr „betrogen“ oder wurde wegen eines verbesserten IKS mehr aufgedeckt? Und wie werden mehr Fälle aufgedeckt: Durch Zufall oder gezielte Abfragen?

Ganz wichtig für uns: Wie sieht der Beitrag des IT-Prüfers aus? Wie kann er den Abschlussrevisor bei der Beurteilung des IKS und den nötigen Tests unterstützen? Und wenn eine Unrechtmässigkeit gefunden wurde: Wie soll dann vorgegangen werden, was gilt als „Beweismittel“? Letzteres ist eine sehr heikle Frage, da die rechtlichen Aspekte im IT-Umfeld grossen Einfluss auf das Vorgehen und die Schlussfolgerungen haben können.

Fragen über Fragen… ich hoffe, liebe Leserinnen und Leser, wir haben Ihr Interesse geweckt und Sie finden die Antworten in den Artikeln in diesem ***NewsLetter***.

Viel Spass beim Lesen

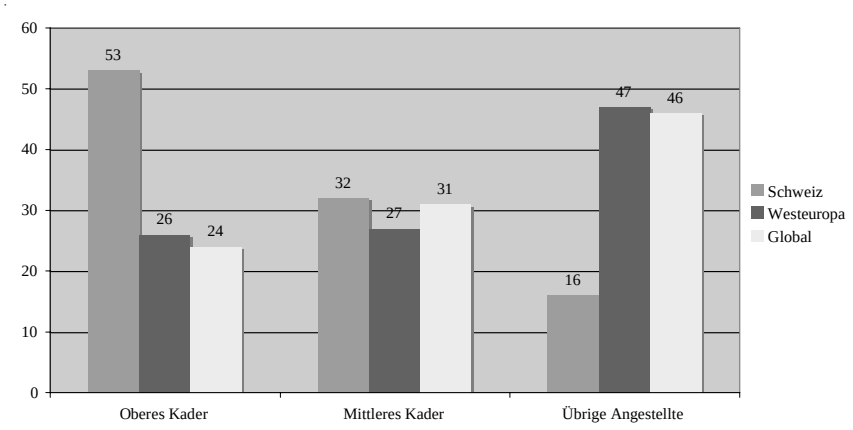
Daniela Gschwend

IT-deliktische Handlungen

Wirtschaftskriminalität in der Schweiz

Das Thema Wirtschaftskriminalität hat spätestens seit den grossen Firmenpleiten in Amerika von Enron und Worldcom eine neue Bedeutung gewonnen. Ein weiteres Beispiel ist der Bankrott der global tätigen und über 200-jährigen Barings Bank, der durch ***einen einzelnen*** Kadermitarbeiter verursacht wurde. Auch in der Schweiz haben Fälle von Wirtschaftsdelikten im höheren Management die Öffentlichkeit aufgerüttelt. Es stellt sich jeweils die Frage, ob der Missstand bzw. der Delikt hätte früher erkannt oder gar vermieden werden?

In einer weltweiten Studie von 2005 [1] hat PWC 3634 Unternehmen in 34 Ländern zur Wirtschaftskriminalität befragt. Für diese Studie wurden von den 1000 grössten Schweizer Unternehmen nach dem Zufallsprinzip 125 Gesellschaften ausgewählt. Davon haben sich 37% als Opfer von Wirtschaftskriminalität zu erkennen gegeben; deutlich weniger als im Vergleich mit 45% weltweit bzw. 43% in Westeuropa. Diejenigen Unternehmen, welche in den letzten zwei Jahren von Wirtschaftskriminalität betroffen waren, verzeichneten in dieser Periode durchschnittlich 5.3 Vorfälle – also rund 245 Delikte in 46 Schweizer Firmen während der letzten zwei Jahre. Das lässt die Frage aufkommen, ob die nicht betroffenen 63% der Schweizer Unternehmen tatsächlich keine Fälle von Wirtschaftsdelikten erlitten haben, diese nicht offen legen wollten, oder sie gar nicht erkannt haben. Hinsichtlich der Position der Täter im Unternehmen ist die Abweichung der Schweiz vom weltweiten Durchschnitt weniger rühmlich:



In der Schweiz ist das obere Kader im Vergleich zu den globalen oder westeuropäischen Ländern überdurchschnittlich häufig als Täterschaft von Wirtschaftsdelikten vertreten. Es stellt sich hier die Frage, ob das Interne Kontrollsystem eines Unternehmens und die Aufsichtsorgane ausreichend wirksam sind, um den sogenannten „Management Override" zu verhindern. Ein Leitfaden zur Vermeidung dieser potentiellen Achillesferse im Internen Kontrollsystem bietet das American Institute of Certified Public Accountants zum Download an [2].

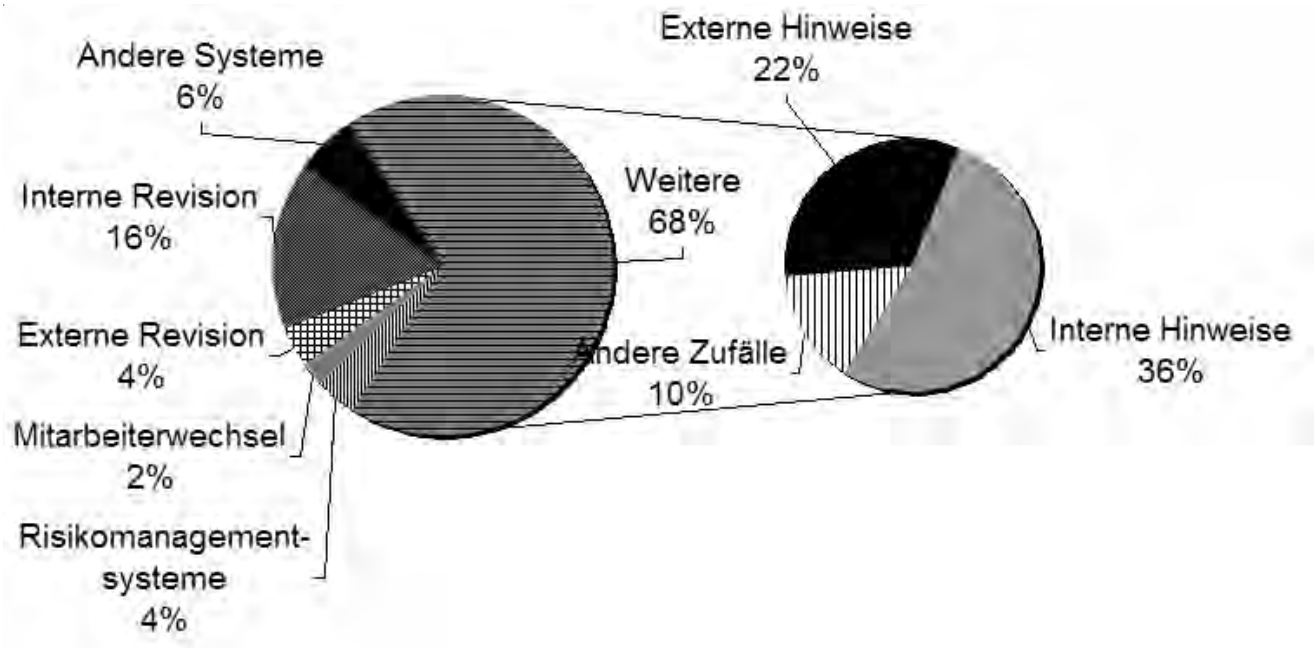
Die drastische Steigerung der gemeldeten Delikte im Vergleich zu 2003 – damals waren es in der Schweiz 24% – werden von den Autoren der PWC-Studie nicht zwingend auf eine Zunahme der effektiven Fälle zurückgeführt, sondern primär auf die folgenden Gründe:

- Verstärktes Bewusstsein und Verständnis für die Auswirkungen von Wirtschaftskriminalität auf den Betrieb sowie eine erhöhte Bereitschaft, einen entdeckten Betrug zu melden.
- Verschärfte Richtlinien innerhalb verschiedener Wirtschaftszweige sowie die effizientere Überwachung durch die zuständigen Aufsichtsorgane.
- Neufokussierung und Anpassung der internen Kontrollsysteme.

Dieser Deutung der Zunahme von 50% in den letzten zwei Jahren möchte ich eine Darstellung der Umfrageergebnisse zur Aufdeckung von Delikten gegenüberstellen.

Aus dieser Grafik ist ersichtlich, dass systematische Massnahmen zur Erkennung von Delikten lediglich 32% der erkannten Fälle an das Tageslicht gebracht haben.

Die Erkenntnis, dass Wirtschaftsdelikte mehrheitlich durch interne oder externe Hinweise aufgedeckt werden, betont die Wichtigkeit und Dringlichkeit der Debatten um die Einführung einer Whistleblower-Hotline in den Unternehmen sowie einer entsprechenden Gesetzgebung zum Schutze der Whistleblower. De facto gibt es seit dem 29. März 2006 eine schweizweite Whistleblower-Hotline, die von Transparency International Schweiz [3] jeden Mittwoch Nachmittag betreut wird. Wissenschaftlich begleitet und ausgewertet wird der Hotlinebetrieb von Profes-



sor Dr. Daniel Jositsch (Leiter des Lehrstuhls für Strafrecht und Strafprozessrecht an der Universität Zürich).

Auch seitens Gesetzgeber ist eine zunehmende Bereitschaft erkennbar, den Schutz der Whistleblower gesetzlich zu regeln. Nachdem die Motion von Remo Gysin zuerst wegen arbeitsrechtlichen Bedenken abgelehnt wurde, wird neu eine abgeänderte Motion der Ständeratskommission vom Bundesrat unterstützt. Das Geschäft geht nun zurück an den Nationalrat.

Luc M. Pelfini, CISA,
Bitterli Consulting AG, Zürich

Quellenangaben:
1 Global economic crime survey 2005 von PWC, sowie länderspezifische Auswertungen in Landessprache (u. A. für Deutschland, Schweiz, England, etc.), www.pwc.com oder Internetsuche nach „global economic crime survey 2005“. Die globale und die deutsche Studie sind zu finden unter www.econcrime.uni-halle.de/ec/global/index.en.php.
2 Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention, American Institute of Certified Public Accountants (AICPA), http://www.aicpa.org/audcommctr/spotlight/achilles_heel.htm
3 Transparency International Schweiz, www.transparency.ch

Weitere empfehlenswerte Quellen zu Wirtschaftskriminalität bzw. der Bekämpfung davon:
- Forensic Computing, fgsec Fachgruppe Security, Auinger/Bitterli/Brunner/et al, kostenlos zu beziehen als pdf-File unter www.isaca.ch
- Kriminalität am Arbeitsplatz, Roger Odenthal, ISBN 3-409-12542-6
- Wirtschaftskriminalität in Deutschland 2003/2004, Umfrage von KPMG, http://www.kpmg.de/library/brochures_surveys/12640.htm

IT-deliktische Handlungen

Computerforensik und Kriminalität

Einleitung[1]

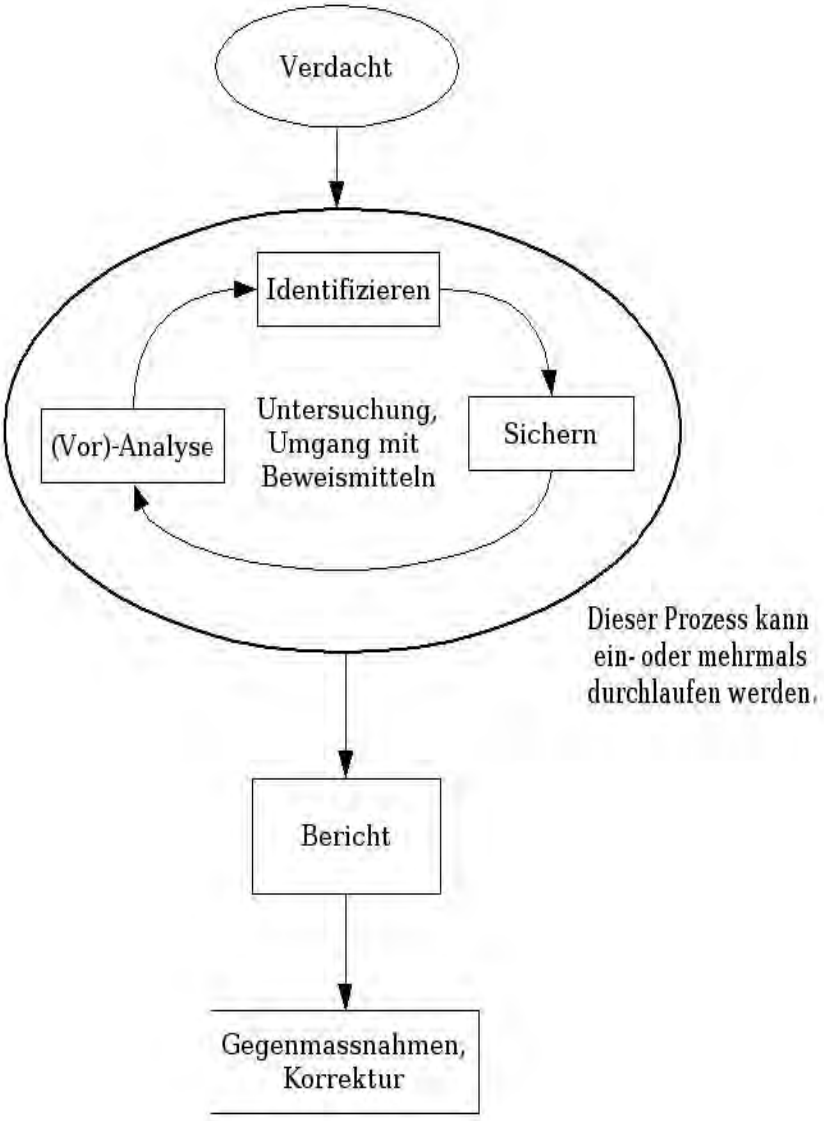
Computer haben schon längst unseren Alltag durchdrungen. Ob Bürofachleute, Privatpersonen, Anwälte, Juristen oder Polizisten, fast jeder benutzt einen PC. So verwundert es nicht, dass es auch immer mehr Computerkriminalität gibt.

Computerkriminelle sind nicht nur unter EDV-Spezialisten zu finden. Auch der durchschnittliche Benutzer kann seinen Computer für kriminelle Zwecke missbrauchen. Statistiken zeigen, dass für bekannte Formen von Kriminalität wie Betrug, Fälschungen usw. vielfach Computer eingesetzt werden.

Die Ermittlung bei Computerkriminalität erfordert spezielle Techniken und Kenntnisse. Computerbasierte Beweismittel sind besonders empfindlich auf unbefugte Änderungen; sei es durch Absicht, durch Unwissenheit oder durch Fehlverhalten. Aus diesem Grund müssen nachweisliche und überprüfbare Vorkehrungen getroffen werden, um die digitalen Beweismittel zu schützen. Dies ist eine der Hauptaufgaben der Computerforensik, wobei die Untersuchungen unter Berücksichtigung der gerichtlichen Verwendbarkeit der Beweismaterialien durchgeführt werden. Dabei kombinieren die Ermittler die strengen Massstäbe der Beweisbehandlung mit den neusten Techniken der Computerwissenschaften.

Forensische Ermittlung

Wie angetönt sind die digitalen Beweismittel von Natur aus sehr verletzlich. Leicht können diese Beweismittel durch absichtliche oder unbefugte Handlungen verändert werden, wobei dies im Nachhinein sehr schwierig nachzuvollziehen ist. Aus diesem Grund werden digitale Beweismittel möglichst nach forensischen Standards untersucht: Nachvollziehbar, nachweisbar und überprüfbar. Um eine Beweiskette aufzubauen müssen Computerforensiker in der Lage sein zu beweisen, dass ihre Kopierverfahren und ihre Analysen die ursprünglichen Daten nicht verändert haben. Daten, die als Beweismittel identifiziert wurden, werden daher vor der eigentlichen Untersuchung mit einem digitalen Fingerabdruck versehen. So kann später überprüft werden, ob die Daten verändert wurden.[2] Ein Kopierverfahren wird üblicherweise auch durch Logdateien protokolliert. Die Beweiskette wird mit einer Dokumentation



Ablauf eine forensischen Untersuchung

aufgebaut, worin jeder Schritt der Beweismittelanalyse beschrieben wird. Logbucheinträge beschreiben die zeitlichen Vorgänge, Formulare beschreiben die Beschlagnahmung und Identifikation der Hardware usw.

Untersucht werden Daten, egal auf welchen Trägern sie gespeichert sind. Typischerweise können dies PC-Festplatten, Disketten, CD-ROM, aber auch ganze Storage Systeme oder mobile Geräte wie Telefone und PDAs sein. Die einzelnen Schritte einer Ermittlung folgen fast immer dem gleichen Muster (siehe Grafik).

Erster Schritt: Identifikation möglicher Beweismittel

Aufgrund eines Verdachts wird eine Untersuchung eingeleitet. Da es während einer forensischen Untersuchung möglich ist, dass spätere Phasen der Ermittlung neue Beweismittel aufdecken, sollten die ersten Schritte dieser Phase möglichst umfangreich sein und genau protokolliert werden. Beispielsweise sollten bei einer Hausdurchsuchung möglichst alle Datenträger mitgenommen werden, auch wenn sich einige nachher als nicht relevant erweisen.

Zweiter Schritt: Sammeln und Sichern von Beweisen

Beweismittel müssen nach forensischen Massstäben kopiert werden. Computerforensiker machen möglichst exakte Kopien der Beweismittel. Dabei wird Datenbit um Datenbit kopiert („Bitstream“). In der Fachsprache heisst diese Art zu kopieren auch „Datenspiegelung“ oder „Klonen“. Mit einem digitalen Fingerabdruck wird anschliessend geprüft, ob die Daten der Quelle mit denjenigen der Kopie übereinstimmen. Stimmen die Fingerabdrücke überein, ist Gewähr, dass der Forensiker eine identische Kopie des Originals in seinen Händen hält, welche die Basis für weitere Untersuchungen darstellt.

Wie geht der Kopiervorgang vor sich? Vorzugsweise „spiegelt“ ein Forensiker einen abgeschalteten Computer, weil dieses Verfahren „reiner“ und übersichtlicher ist. Das Erheben der Beweise bei noch laufenden Rechnern ist komplizierter und birgt viele Fallstricke für die forensische Beweissammlung. Ein gehackter Computer sollte jedoch nicht ordnungsgemäss heruntergefahren werden, da ein Hacker Löschprogramme hinterlassen haben könnte, die dann aktiv werden. Das Untersuchungsobjekt könnte auch ein Firmenserver sein und ist möglicherweise zu wichtig, um heruntergefahren zu werden. Ausserdem kann das Beweismittel auch im Arbeitsspeicher liegen und würde daher nicht auf dem Datenträger aufgefunden werden. So muss der Ermittler eine Priorisierung durchführen und die Beweismittel in der Reihenfolge ihrer Gefährdung (auch Flüchtigkeit) kopieren. Allenfalls muss danach der Stromstecker des Computers herausgezogen werden, um mögliche Folgeschäden oder das Löschen von Beweisen zu verhindern. Das Kopieren von Arbeitsspeichern ist aus forensischer Sicht besonders heikel, da der Kopiervorgang auch Spuren im Arbeitsspeicher hinterlässt (das Kopierverfahren selber ist ein Prozess, der Speicher benutzt). Somit ist es unvermeidbar, dass Beweismittel während man sie sichert verändert werden. Ein digitaler Fingerabdruck kann beweisen, dass die Daten wenigstens seit dem Sammeln nicht geändert wurden. Ein solcher Vergleich mit dem Zustand der Quelle vor und nach dem Kopieren wird aber hier fehlschlagen.

Dritter Schritt: Voranalyse und Analyse

Die Kopien der ursprünglichen Datenträger werden im Anschluss auf Spuren untersucht und ausgewertet. Eine Voranalyse überprüft die Vollständigkeit des Beweismaterials. Öfters kommen auch andere Spuren zum Vorschein, welche das Vorgehen der Computerforensiker beeinflussen. Bei dem erwähnten Beispiel der Hausdurchsuchung werden alle Datenträger beschlagnahmt, aber vielleicht zuerst nur die PC-Festplatte analysiert. Wenn dort Hinweise auf CD-ROM oder Disketten gefunden werden, werden die betreffenden Datenträger natürlich dupliziert und analysiert. Die ersten drei Schritte einer Untersuchung (vgl. vorstehend) können sich deswegen wiederholen bis eine ausreichende oder vollständige Beweislage vorhanden ist. Weil es sich hier um ein heuristisches Verfahren handelt, ist die Abgrenzung zwischen der Voranalyse und der eigentlichen Analyse oft fliessend.

Spuren werden nicht absichtlich hinterlassen, aber auch nicht immer absichtlich verwischt. Computerforensiker benutzen spezialisierte Hardware und Programme, um diese Spuren zu finden und zu analysieren. So kann der Forensiker Beweise in gelöschten Dateien, Datenfragmenten (teilweise überschriebene Dateien), unbenutzter Speicherplatz (z.B. „slack space“) oder in Meta-Daten von Anwendungen (z.B. Word, Excel) auffinden. Das Ziel einer forensischen Untersuchung ist es, Klarheit über die Aktivitäten eines möglichen Täters zu erhalten.

Vierter Schritt: Dokumentieren

Die gefundenen Beweise werden unter Umständen während eines Gerichtsverfahrens diskutiert und ausgewertet. Die Beschreibung der

Resultate, die Dokumentation des Vorgehens für den Beweismittelschutz sowie der Analyse können eine Ermittlung glaubwürdig oder unglaubwürdig erscheinen lassen. Zusätzlich ist es die Pflicht eines Computerforensikers, die komplexen technischen Vorgänge für Laien verständlich und nachvollziehbar zu beschreiben.

Die Computerforensik ist ein relativ neues Gebiet, worin eine Kombination von forensischen Verfahren mit technischem IT-Wissen und der traditionellen Spürnase eines Ermittlers verlangt wird. Zudem wächst die Komplexität der Computerkriminalität, wegen der schnellen internationalen Verbreitung des Wissens über kriminelle Methoden und Verfahren, ständig. Deshalb muss der Ermittler immer am neusten Stand der Entwicklungen dranbleiben und sich weiterbilden.

Problem Computerkriminalität

Die folgenden Beispiele geben eine kleine Übersicht über den Umfang des Problems Computerkriminalität:

- 1988 berichtete das amerikanische Computer Emergency Response Team CERT/CC über sechs Fälle von Computerkriminalität. Im Jahre 2002 waren es bereits 82'094 und 2003 137'529 Fälle.[3] Die CSI/FBI Computer Crime and Security Survey bezifferte den Gesamtverlust durch Computerkriminalität für 2003 auf rund USD 202 Mio. Angriffe fanden gemäss der Studie hauptsächlich über das Internet statt.[4]
- In Deutschland verfasst das Bundeskriminalamt (BKA) jährlich die polizeiliche Kriminalstatistik (PKS), welche aber nur abgeschlossene Verfahren beschreibt. Dies sind nur die Fälle, die der Polizei gemeldet wurden. Spezialisten rechnen zudem mit einer massiven Grauzone von nicht deklarierten Delikten. Von 3067 Fällen in 1987 stieg die Zahl auf 79'283 in 2001. Die PKS von 2002 zählt 40'346 Fälle von betrügerischer Ausnutzung des Lastschriftverfahrens (Debitkarten ohne PIN) nicht zur Computerkriminalität. Fügt man diese wieder hinzu, kommt man auf 97'834 Fälle, was einen Zuwachs von 23% gegenüber dem Vorjahr bedeutet.[5]
- Die PwC Global Economic Crime Survey 2003 gibt Informationen über die Lage in der Schweiz. Computerkriminalität war mit 15% weltweit die drittgrösste Form von Wirtschaftskriminalität (nach Veruntreuung mit 60% und Produktediebstahl mit 19%). In der Schweiz nimmt die Computerkriminalität mit 20% den zweiten Platz ein (nach Veruntreuung mit 60%). Firmen erwarten die grössten zukünftigen Gefahren bei der Veruntreuung (35%) gefolgt von Computerkriminalität (31%).[6]

Mark Furner, Compass Security, Rapperswil

Referenzen

[1] Dieser Artikel basiert auf dem Artikel „First Forensic Forum Schweiz (F3-CH) Computerforensik und Computerkriminalität" publiziert in „Recht", 05/2004, S. 210-212, http://www.recht.ch/

[2] Digitale Fingerabdrücke sind numerische Werte, die durch einen Algorithmus anhand des Inhalts einer Datei erstellt werden. Diese Werte sind gross genug, um eineindeutig zu sein. Nach der Erstellung eines digitalen Fingerabdrucks kann man nachweisen, ob die Daten geändert wurden, weil der Algorithmus dann einen anderen Fingerabdruck-Wert berechnet, oder den selben Wert ermittelt. Dieser Wert, auch Prüfsumme genannt, wird so Bestandteil einer digitalen Beweiskette und bürgt für Integrität der Daten.

[3] http://www.cert.org/stats/cert_stats.html

[4] Der Bericht kann über http://www.gocsi.com/press/20030528.jhtml bezogen werden.

[5] http://www.bka.de/pks/zeitreihen_2002/pdf/t01.pdf und http://www.bka.de/pks/pks2002/index2.html

[6] Bezugsquelle für den Bericht: http://www.pwcglobal.com/ch/ger/ins-sol/publ/cfr/crime_survey.html

Hilfe bei Compass Security

Compass Security verfügt über umfangreiche Erfahrungen auf dem Gebiet der Netzwerksicherheit sowie dem Hacking, forscht aktiv nach neuen Angriffs- und Testmethoden und programmiert eigene Werkzeuge für professionelle Security Assessments. Dank dem spezifischen Know-how konnte Kunden schon oft Unterstützung bei Ermittlungen geboten werden.

Compass Security beschäftigt sich seit April 2004 professionell mit dem Thema Computer Forensik. Dank kompetenten Fachpersonen und der notwendigen Hard- und Software können Gutachten für Justiz und Wirtschaft erstellt werden.

Mehr Informationen über Compass Security und unsere Dienstleistungen finden Sie unter: http://www.csnc.ch

Über den Autor

Mark Furner ist promovierter Historiker und Computerforensiker. Nach einer Ausbildung als Programmierer und Analytiker auf IBM Grossrechnern ist er seit 2000 in der Computerforensik tätig und hat Untersuchungen für die Justiz und Wirtschaft durchgeführt. Seit Juni 2004 arbeitet er bei Compass Security und ist Mitautor der Inhalte des dreitägigen ISACA Evidence Lab-Seminars. Der Kurs vermittelt das Wissen rund um die Beweismittelführung und -Verwertung. Eine Broschüre über das ISACA Evidence Lab finden Sie unter folgender URL: www.csnc.ch/static/services/training/esl.html

IT-deliktische Handlungen

Prüfungsstandard 240

Bei Aufnahme meiner Tätigkeit als Revisionsassistent Mitte des letzten Jahrhunderts sagte mein erster Chef zu mir: „Merken Sie sich: Ein Revisor glaubt zuerst einmal nichts, ausser, dass alle Buchhalter Betrüger sind." Als er mein entsetztes Gesicht sah, fügte er hinzu: „Abgesehen von denen, die aus lauter Dummheit Fehler machen." Mein damaliger Chef war der Überzeugung, sein Lebenswerk bestehe darin, Fehler aufzudecken und betrügerische Buchhalter ins „Chefi" (wie er es nannte, für Nichtschweizer Gefängnis) zu bringen.

Der Ausspruch kam mir wieder in den Sinn, als ich mir den Titel des PS 240 in die Birne zog: ***Deliktische Handlungen und Fehler – Verantwortung des Abschlussprüfers***. Längst hatte ich begriffen, dass mein damaliger Chef masslos übertrieben hatte. Dennoch war der Nagel eingeschlagen, und als ich meine späteren Vorgesetzten darauf hinwies, dass die Revisoren sehr wohl eine gewisse Verantwortung bezüglich der Aufdeckung von Delikten hätten, wurden mir „die Nähte" ein getan: Das dürfe ich auf keinen Fall sagen, denn es könnte daraus eine Verantwortung der Revisionsstelle abgeleitet werden. Vielmehr sei es die Aufgabe des Prüfers, unter die Jahresrechnung seinen Haken zu setzen. Und damit basta.

Die Philosophie bezüglich der Verantwortung des Prüfers wandelte sich im Laufe der Zeit. Ende des Jahrtausends ging sie aus meiner Sicht so weit zu unterstellen, dass die Unternehmen darauf ausgerichtet seien, Gewinn zu erzielen; es sei daraus abzuleiten, dass sie ein Interesse daran hätten, den Sachverhalt der Finanzlage richtig darzustellen. Denn die Buchhaltung sei das wichtigste Führungsinstrument überhaupt. Falsche Unterlagen müssten demnach zu falschen Entscheiden führen, und dies sei nicht im Interesse des Unternehmers. Deshalb sei zu unterstellen, dass die Buchhaltung grundsätzlich richtig sei. So etwas wie eine Unschuldsvermutung vor Gericht. Wenn jeweils diese Meinung ***in extremis*** vertreten wurde, drehte es mir beinahe den Magen um.

Enron, ***Parmalat, Worldcom*** und viele anlässlich gewissenhaft durchgeführter ***Due Diligence*** Prüfungen entdeckter Unstimmigkeiten haben uns inzwischen eines Besseren belehrt. Es sind nicht nur die kleinen Hilfsbuchhalter, welche Fehler begehen. Immer wieder ist es die obere Etage, welche durch ***Management Override*** finanzielle Darlegungen zu verfälschen versucht.

Nun. Ist es denn die Verantwortung des Prüfers, Fehler und deliktische (strafrechtlich relevante) Handlungen aufzudecken? Die Einleitung des PS 240 scheint diese Frage zu verneinen: „…primär liegt … die Verantwortung für die Verhinderung bzw. Aufdeckung von deliktischen Handlungen und Fehlern bei den Verantwortlichen für die Leitung und Überwachung … eines Unternehmens." Gleich darauf folgend wird aber fett festgehalten: „Bei der Planung und Durchführung von Prüfungshandlungen, den Schlussfolgerungen daraus sowie der Berichterstattung muss der Abschlussprüfer das Risiko in Betracht ziehen, dass der Abschluss wesentliche Fehlaussagen infolge von deliktischen Handlungen und Fehlern enthält." Also doch.

PS 240 nennt u.a. folgende Möglichkeiten, bei welchen Fehler und deliktische Handlungen auftreten können: Fehlerhafte Erfassung und Verarbeitung von Daten; nicht angemessene Schätzung; unrichtige Anwendung von Rechnungslegungsgrundsätzen; Manipulationen, Fälschungen; unrichtige Darstellung von Ereignissen; Veruntreuungen.

Und was bedeutet das Ganze jetzt für den IT-Revisor? M.E. sollte er bei der Planung und Durchführung von Prüfungshandlungen in folgenden Bereichen mitwirken, wobei eine sorgfältige Risikoanalyse die anfälligen Bereiche voranzustellen ist:

Fehlerhafte Erfassung von Daten

An dieser Stelle entstehen Fehler in erster Linie durch mangelhaftes IKS. Wozu aber braucht man einen IT-Spezialisten zur Beurteilung des IKS?! Viele Massnahmen des IKS sind in den heutigen IT-Systemen integriert. Als Beispiel gelte das Vieraugenprinzip. Frage: Wurde es hinreichend in die Erfassungsprogramme (z.B. durch Freigabevisum) umgesetzt? Diese Antwort kann der IT-Revisor durch Studium der Dokumentation und Ausführen eigener Tests geben. Gleiches gilt bezüglich des Einbaus aller Arten von Plausibilitäten in den Erfassungsprogrammen.

Wenn die Programme an sich eine fehlerhafte oder deliktische Erfassung nicht verhindern können, ist der Einsatz von ***Audit Software*** in Erwägung zu ziehen. Dadurch können z.B. auffällige „Ausreisser" oder Häufigkeiten aufgedeckt werden.

Fehlerhafte Verarbeitung von Daten

Hier sind zwei Arten von Fehlern bzw. Manipulationen zu unterscheiden. Erstens kann ein Programm systematisch falsch arbeiten. Als Beispiel gelte hier die viel zitierte Abrundung in einem Zinsberechnungsprogramm. Zweitens kann ein Programm während der Ausführung durch einen Operator beeinflusst werden. Im ersten Fall gelten wiederum die Tätigkeiten des Dokumentationsstudiums und der Tests; im zweiten die Überprüfung des IKS im Umfeld der Computerverarbeitung, allenfalls auch die Analyse von Logs.

Nicht angemessene Schätzung

Wenn es sich um IT-verwandte Schätzungen handelt (z.B. Softwarebewertung) kann der IT-Revisor auch hier wertvolle Hinweise geben.

Unrichtige Anwendung von Rechnungslegungsgrundsätzen

Analog der fehlerhaften Erfassung und Verarbeitung von Daten geht es wohl um die zutreffende Umsetzung von Regeln in Programmen. Deshalb gelten hier die gleichen Bemerkungen. Als Kundiger auf den Gebieten der Revision und der IT wird der IT-Revisor die korrekte Interpretation der Verarbeitungsregeln beurteilen können.

Manipulationen und Fälschungen

Sie erfolgen bei Eingabe, Verarbeitung und/oder Ausgabe der Daten, also bei den Grundelementen der IT! Ob solche überhaupt möglich sind, wird der IT-Revisor bezüglich der IT-Prozesse sehr wohl einschätzen können. Erfolgen sie ausserhalb der IT, ist er wahrscheinlich überfordert. Vielfach allerdings auch der konventionelle Revisor… Daneben könnte der Einsatz von ***Audit Software*** an dieser Stelle zum Aufdecken von Manipulationen und Fälschungen beitragen.

Unrichtige Darstellung von Ereignissen

Entweder liegt ein Fehler infolge mangelhaften IKS oder ein ***Management Override*** vor. Demnach kann eine Untersuchung des IKS die eine Fehlerquelle eliminieren helfen, wobei ein Zusammenarbeiten mit der konventionellen Revision unabdingbar ist. Erfolgt der ***Management Override*** unter Beeinflussung der IT (z.B. Operating), kann eine Untersuchung des IT-Umfeldes eine solche Manipulation verhindern oder aufdecken. ***Audit Software*** kann zusätzlich beitragen, eine solche Fehlinstruktionen (Storni, Wiederholungen von Verarbeitungen, usw.) aufzudecken.

Veruntreuungen

Sie erfolgen oft über das Kreditorenwesen. Entweder werden Zahlungen an Adressen veranlasst, die es eigentlich gar nicht geben sollte, oder es werden zu hohe Zahlungen veranlasst, um via ***Kickback*** die Geldmittel zu erlangen. Einmal mehr sind die Stichworte IKS (Mutationswesen) und ***Audit Software*** gefragt.

Der PS 240 ist ein weiteres Beispiel dafür, dass der IT-Revisor nicht nur bei der Durchführung, sondern auch bei der Revisionsplanung der Abschlussprüfung, ein gewichtiges Wort mitsprechen sollte.

Max F. Bretscher, Langnau a/A

Eine Revisorin hatte auf ihre Standhaftigkeit gebaut,
Und zudem den kräftigen Virusbeschützern vertraut.
Das Alarmsystem war völlig vernetzt,
Sie wurde dennoch schäbig verletzt:
Ihre Ehre und auch das Computersystem wurden geklaut.

An eager young audit assistant with the name Maud
Measured her communication links always in Baud.
She thought to be very speedy
But her colleagues were greedy.
In the end her connections turned out to be fraud.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Sécurité TEI

Éléments critiques pour la réussite d'un programme de sécurité des informations

Le projet de l'IT Governance Institute (ITGI)

Ayant constaté que peu de documents identifiaient d'une manière compréhensible les éléments critiques pour la réussite d'un programme de sécurité des informations et les pistes de solutions pour résoudre les obstacles sous-tendus, l'ITGI a décidé de créer un projet pour combler ce vide.

Les buts de ce projet étaient les suivants :

- Fournir aux Responsables de la Sécurité des Informations une perspective des éléments critiques pour la réussite d'un programme de sécurité des informations,
- Fournir des suggestions de solutions des problèmes sous-tendus,
- Fournir un rapport qui puisse être utile non seulement aux Responsables de la Sécurité des Informations mais aussi au Comité Exécutif et au Conseil d'administration.

Pour ce faire, un groupe de dix experts en Sécurité des informations a été créé. Comme on peut le constater, ce groupe de spécialistes représente divers types d'activité ainsi que différentes géographies. Afin d'avoir une rédaction du rapport homogène, la rédaction du rapport a été confiée à Sharon K. O'Bryan.

La première tâche de ce groupe a été de définir une liste d'éléments considérés comme critiques par ce groupe. Trente-cinq éléments ont ainsi été répertoriés.

Afin de déterminer les dix éléments les plus critiques de cette liste, elle a été soumise à deux votes en parallèle:

- Un vote du groupe de travail,
- Un vote d'un échantillon représentatif de Responsables de la Sécurité des Informations.

Pour le deuxième vote, la liste a été envoyée à 800 personnes et 157 d'entre elles ont répondu. Il est intéressant de noter que parmi les dix choisis, les deux votes ont sélectionné les mêmes six éléments.

Avec ces résultats, le groupe de travail a proposé pour chacun des quatorze éléments des pistes de solutions.

Le rapport

Le résultat de ces travaux fait l'objet d'un rapport qui doit être publié par l'ITGI au début de l'année 2006. Les six éléments les plus critiques sont :

- L'engagement de la Direction dans les initiatives relatives à la sécurité des informations,
- La compréhension par la Direction des problèmes relatifs à la sécurité des informations,
- La planification de la sécurité des informations avant l'introduction de nouvelles technologies,
- L'intégration des métiers et de la sécurité des informations,
- L'alignement de la sécurité des informations avec les objectifs de l'entreprise,
- L'appropriation et la responsabilisation de la Direction et des responsables métiers vis-à-vis de l'implémentation de la sécurité des informations, la surveillance des mesures et la remontée des informations relatives à la sécurité des informations.

Les huit éléments additionnels sont :

- Une éducation appropriée des employés sur la protection des biens informationnels,
- Une mise en application cohérente des politiques et standards de sécurité des informations,
- L'emplacement de la sécurité des informations dans la hiérarchie de l'entreprise,
- Le budget pour la stratégie et la tactique de la sécurité des informations,
- L'existence de messages cohérents relatifs à la sécurité des informations en provenance de la Direction,
- Une focalisation sur des objectifs à court terme entraînant des faiblesses à long terme,
- La capacité à justifier les coûts de la sécurité des informations,
- L'existence de tableaux de bord normalisés.

Pour chacun de ces quatorze éléments, on trouve une description de ces éléments, des propositions de solutions destinées à la direction et des propositions de solutions destinées aux Responsables de la Sécurité des Informations.

L'information contenue dans ce rapport montre clairement que la sécurité des informations n'est pas seulement un problème de la direction des systèmes d'information mais surtout un problème métier.

L'aptitude à identifier convenablement les risques qu'encourent les

biens informationnels nécessite la semble aussi important que la coopération de toute l'entreprise.

Il semble aussi important que la Direction et les Responsables de la Sécurité des Informations forgent des relations qui permettent de communiquer un message clair sur la priorité que l'entreprise accorde à la protection des biens informationnels. De plus, il faut que ce message soit soutenu par des actions visibles et cohérentes.

Il importe aussi que les conflits de priorités au sein de l'entreprise ne mettent pas constamment en attente la sécurité des informations. En effet, les résultats de cette étude indiquent que sans un engagement, une définition et une attention persistante de la direction sur la sécurité des informations, la protection des biens informationnels continuera d'être sujet à des implémentations « urgentes » mettant de côté les standards, politiques et procédures et conduisant à saper l'infrastructure technologique de l'entreprise.

Il apparaît aussi que le rôle des Responsables de la Sécurité des Informations est en évolution. En effet, leurs décisions demandent une compréhension des risques métiers, une connaissance des métiers de l'entreprise et une interaction croissante avec les départements légaux et conformité aux lois et règlements. Il convient donc d'évoluer d'un métier essentiellement technologique vers un métier orienté gestion de l'entreprise.

En conclusion, s'il n'y avait qu'une chose à retenir c'est que les biens informationnels continuent d'être à risque avec la communication et l'engagement de la Direction à l'épicentre des programmes de Sécurité des Informations.

Yves Le Roux, Computer Associate

Repris avec la permission de ISACA international

ISACA Serving IT Governance Professionals Switzerland Chapter

www.isaca.ch

Unsere aktuellen Kurse!

ITIL Foundation Training
Service Management auf der Basis des de-facto Standards ITIL
7. – 9. Juni 2006 in Zürich

BS 15000 und ISO 20000 Consultant & Internal Auditor
Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung
12. – 14. Juni 2006 in Zürich

ITIL Foundation mit Apollo 13
inkl. int. Zertifizierung
28. – 30. Juni 2006 in Zürich

SAP R/3 für Wirtschafts- und Informatikprüfer
Lernen Sie, im SAP R/3 Umfeld Geschäftsprozesse effizient und wirksam zu prüfen.
13. – 15. September 2006 in Stuttgart
Einführungstag 12. September 06, Stuttgart

Content und Mobile Security Lab
Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung
27. – 29. September 2006 in Zürich

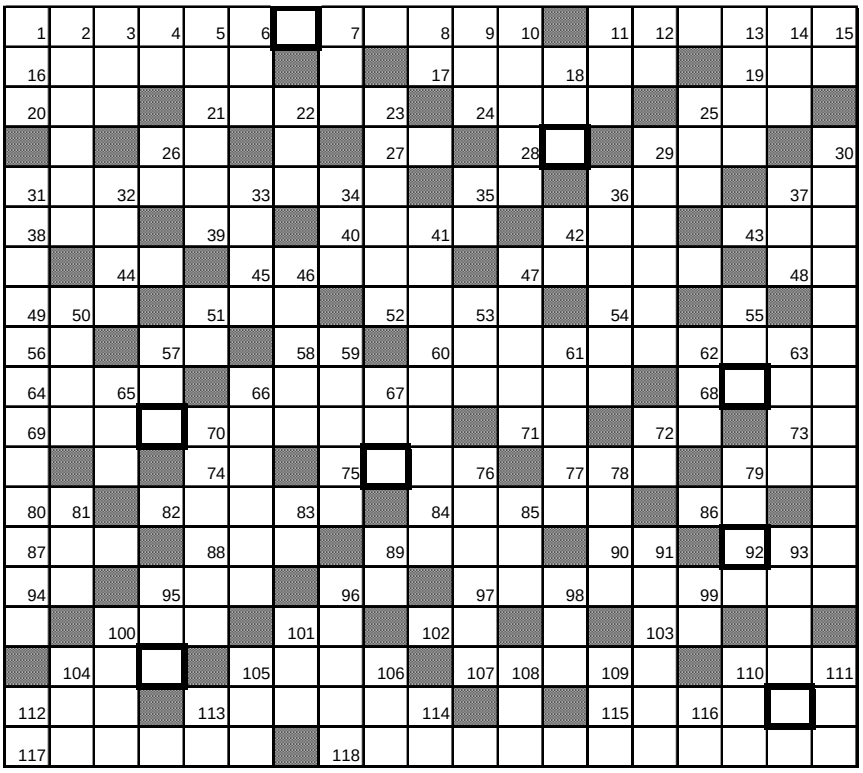
Weitere Informationen erhalten Sie in unserem Kurssekretariat

ISACA Switzerland Chapter
c/o ITACS Training AG, Stampfenbachstrasse 40, 8006 Zürich, Schweiz, kurse@isaca.ch, Tel. 044 444 11 01, Fax 044 444 11 02

ISACA
Serving IT Governance Professionals
Switzerland Chapter

The ISACA Crossword Puzzle 2/06

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 ***Nötigung*** (Mz); 11 indischer Strom; 16 mit Kaul davor ein potentieller Frosch; 17 Furche; 19 Insel (frz); 20 kurzes Übermittlungszentrum; 21 Bewohner des Zweistromlandes (Mz); 24 Blutbahn; 25 schön (frz); 26 eisernes Kreuz; 27 ägypt Sonnengott; 28 European Community; 29 Fragewort; 31 ***Schwindler***; 35 Jugendlager; 36 Fluss (span); 37 Maine; 38 eine (frz); 39 kurze Rechnung; 40 alle (j=i); 42 griech Hirtengott; 43 lediglich; 44 gehen (span); 45 afrikanischer Stamm; 47 lustiges Fest; 48 AZ Sowjetunion; 49 Rain; 51 Welle (span); 52 Geliebte des Zeus; 54 Vorname der Derek; 56 AZ aus der Ostschweiz; 57 Vorwort; 58 Leutnant; 60 ***Missetäter***; 64 rückwärts doppelter Eselslaut; 66 ***imitieren***; 68 teuer (frz); 69 Beweglichkeit; 71 Anschrift an Unbekannt; 72 Ausruf der Bewunderung; 73 König (it); 74 in Ordnung; 75 Madrider Sportclub; 77 weibl Nutztier; 79 Seil; 80 sechste Tonstufe; 82 sagenhafte Schneemenschen; 84 Wildschweinzähne; 86 Flussname aus der Innerschweiz; 87 Bindewort; 88 pers Fürwort; 89 Tide; 90 eingetragener Verein; 92 der grosse steht in London; 94 AZ aus der Westschweiz; 95 kurzes Revier; 96 deutsche Vorsilbe; 97 ***hat schon mancher 60 waagrecht versprochen***; 100 Barbies Liebling; 101 nach dem Grounding untergegangen; 102 aromatisches Getränk (span); 103 zwei gleiche Konsonanten; 104 erster Sekretär der UNO; 105 Spaltwerkzeug; 107 rein; 110 jap Münze; 112 Vorname der West; 113 Jahreszeit; 115 Schiff sichern; 117 vornehmes Schloss; 118 ***Veränderung***.

Senkrecht: 1 kurzes gleich; 2 ***tadeln***; 3 Friede (span); 4 schweiz Scheidemünze; 5 griech Philosoph; 6 sein (span); 7 Witz; 8 zwei gleiche Konsonanten; 9 Zeitabschnitt (it); 10 Nähwerkzeug; 11 Wurfspeer; 12 Vorwort; 13 Verlangen; 14 engl Längenmass; 15 Südost; 18 Schnabel (frz); 22 ***bös***; 23 unwirklich; 25 sprechender Vogel; 26 pers Fürwort; 29 ***solches Dressing ist verpönt***; 30 ***unredlich Geld beiseite schaffen***; 31 Bibliothek; 32 träge Masse; 33 gleich; 34 Gefrorenes; 35 pers Fürwort (frz); 36 ***mit Gewalt aneignen;*** 37 Brei; 41 ***Klauvorgang***; 42 kurzer Vater; 46 Kaltspeise; 47 Ausdruck der Langeweile in einer Wortblase; 50 Aufgeld; 51 Einschaltknopf; 53 kurzer engl Mediziner; 55 Zischlaut; 57 römisch drei; 59 Tränen (engl); 61 Schnitterwerkzeug; 62 pers Fürwort; 63 Gattin des Zeus; 65 Klostervorsteher; 66 ***erfunden***; 67 Windseite; 70 entwinden; 72 Flusslandschaft; 76 Altanen; 78 griech Kriegsgott; 79 Verbotenes; 81 Esel (frz); 83 Dehnlaut; 85 Nibelungenmutter; 89 CZ Eisen; 91 Stadt in Norditalien; 93 ganz (it); 95 Wendekommando; 96 märchenhafte Brüder; 98 Zusammengehöriges; 99 an amerikanischen Bahnübergängen zu sehen; 100 Schiffsteil; 101 Sohn Noahs; 104 Ort an der Thaya; 105 Unrat; 106 die Kuhgesichtige; 108

Standardsoftware (Abk); 109 Senke; 110 Befehlsform von sein; 11 drei gleiche Konsonanten; 112 Maschinenpistole; 113 Schutzstaffel; 114 registered nurse; 116 Anfang und Ende von Kent.

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 12. Januar 2006.

Solution Crossword Puzzle 1/06: REPORTINGS

Across: 1 ***balances***; 9 ***purpose***; 15 intrinsic; 18 pea; 19 as; 20 H(er) M(ajesty's) S(ervice); 21 rot; 23 CRS; 24 is; 25 ***workfiles***; 28 take; 29 SA; 30 isla; 31 bat; 32 ***auditor***; 34 apt; 36 copt; 38 orb; 39 SE; 40 Mubarak; 42 Ei; 43 Sabo; 45 es; 46 or; 47 Klara; 49 aeri(al); 50 ***experts***; 51 Emil; 52 snuff; 54 te; 55 ay; 56 esos; 57 sa; 58 firecat; 60 BT; 61 rat; 61 Ulme; 64 cri; 65 illegal; 67 Erz; 68 NATO; 70 il; 72 aces; 73 ***balancing***; 77 Po; 78 net; 80 l(i)t(e)r; 81 tar; 82 CS; 83 get; 85 yardstick; 89 essence; 90 hesitate.

Down: 2 ***aims***; 3 Lns; 4 at; 5 NRMO (Norm); 6 ci; 7 Enak; 8 SS; 10 up; 11 red; 12 Pa; 13 (Cutty) Sark; 14 ***essential***; 16 iris; 17 ***collaboration***; 20 hit; 22 teaparty; 25 wad; 26 rate; 27 firmspecialty; 28 tackles; 29 Subaru; 32 Arsenal; 33 ISO; 37 TR; 37 peris(t)al; 41 AK; 44 biffers; 45 ***external***; 48 amoral; 49 ***assurance***; 53 FI; 56 été; 59 RC; 60 Blei; 63 meet; 66 gig; 69 tara; 71 for; 73 cess; 75 code; 76 Nati; 77 Pakt; 79 hen: 81 TCA; 84 GE; 84 TC; 55 Rh(esus); 87 ss; 88 ***IT***.

Watson: The solution is in squares without a number.

Es trafen weniger als fünf richtige Einsendungen ein.

Im Jackpot sind somit US$ 100.

IT-Tagung 2006

Aktuelle Entwicklungen, Methoden, IT-Sicherheit, Tools und Technik

Vom **22.-23.Mai 2006** in Frankfurt

Themen:
- Cobit 4.0 – ein neuer Meilenstein oder nur ein Update
- ISO 27001 Implementierung mit IT-Grundschutz
- The Impact of ITIL on IT Audits
- ISO 20000 – Die Zertifizierung für IT(IL)- Organisationen
- Aktivitäten des FAIT beim IDW
- Prüfen und Testen von Software – Prozesse und Methoden
- Prüfung von IDV und End-User-Developments am Beispiel der Office-Produktpalette
- Computer Forensik
- Audits in SAP-Systemen
- IT-gestützte Berechtigungsprüfung in SAP R/3
- Effektivität und Effizienz aufdeckender IT-Kontrollen
- Sicherheit und Prüfung in vernetzten Systemen
- PKI / Digitale Signatur
- Joint Audits – Zusammenspiel IT- und Fach-Audit
- Komplexität vernetzter Systeme – Sicherheit und Prüfbarkeit

Weitere Infos unter:
Deutsches Instituts für Interne Revision e.V. (IIR)
Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69-0
Telefax (069) 71 37 69-69
http://www.iir-ev.de

Express Line

A Word From the Chair

Greetings! As you are aware, the annual ISACA membership purge takes place each April. After the purge, members who have not yet renewed with ISACA International Headquarters will no longer receive member benefits, including the ***Information Systems Control Journal®*** and access to K-NET® and all member-protected areas of the ISACA web site.

Steve Thorsted
Chair, Membership Board

Reminder to Participate

ISACA members interested in serving during the next administrative term may apply via the Invitation to Participate brochure.

Participation benefits not only the association and its members as a whole, but also the participant as an individual and professional. Some benefits and opportunities provided to participants include:

- Networking with colleagues internationally
- Impacting ISACA services and deliverables
- Being a part of an active, seasoned volunteer team
- Enhancing work experience

The Invitation to Participate brochure (for key board/committee service) was mailed with volume 1 of the ***Journal*** and is available for download from the ISACA web site at ***www.isaca.org/participate***.

Bookstore Update

Preparing for the 2006 Certified Information Systems Auditor™ (CISA®) or Certified Information Security Manager® (CISM®) exam? The CISA and CISM study aids published by ISACA are now available for the 2006 exams.

2006 CISA Exam

Reference Material

- ***CISA Review Manual 2006*** (English, Italian, Japanese and Spanish editions available)
- ***CISA Review Questions, Answers & Explanations*** CD-ROM 2006 (725 questions) (English and Spanish editions available)
- ***CISA Review Questions, Answers & Explanations Manual 2006*** (625 questions) (English, Italian, Japanese and Spanish editions available)
- ***CISA Review Questions, Answers & Explanations Manual 2006 Supplement*** (100 questions) (English, Italian, Japanese and Spanish editions available)

2006 CISM Exam

Reference Material

- ***CISM Review Manual 2006*** (available in English only)
- ***CISM Review Questions, Answers & Explanations Manual 2006*** (200 questions) (English and Japanese editions available)
- ***CISM Review Questions, Answers & Explanations Manual 2006 Supplement*** (100 questions) (available in English only)
- ***CISM Review Manual 2005*** (English and Japanese editions available)
- ***CISM Review Questions, Answers & Explanations Manual 2005*** (100 questions) (available in Spanish only)

Descriptions and ordering information are available at ***www.isaca.org/cisabooks*** for CISA study aids, www.isaca.org/cismbooks for CISM study aids, and www.isaca.org/nonenglishbooks for CISA and CISM study aids in non-English languages. Please contact the ISACA Bookstore at +1.847.253.1545, ext. 401 or 478, or e-mail bookstore@isaca.org, with any questions.

CISA and CISM Exam Highlights

June 2006 Exam Deferrals

Members unable to take the exam can request a deferral of their registration fees to the next exam date. Those requests received on or before 1 May 2006 will be charged a US $50 processing fee. From 2 May 2006 through 2 June 2006, a processing fee of US $100 will be charged. Deferral requests will not be accepted after 2 June 2006.

For the convenience of ISACA members, a deferral can now be requested online at www.isaca.org/examdefer. Should your members have additional questions concerning cancellations or deferrals, please have them contact the certification department at certification@isaca.org or +1.847.253.1545, ext. 403, 471 or 474.

DACH-News

In eigener Sache

Aus Deutschland erreicht uns im Februar 2006 ein e-mail mit folgendem Inhalt:

„Sehr geehrte Frau Josi,

Nach langen Jahren der Kooperation zum Thema ***NewsLetter*** mit dem Schweizer Chapter hat der Vorstand des Deutschen Chapters beschlossen, eine eigenständige Publikation für Deutschland ins Leben zu rufen. Aus diesem Grunde möchten wir unsere ***NewsLetter-***Kooperation mit dem Schweizer Chapter gern zur Jahresmitte beenden … Ingo Struckmeyer, Vorstand Publikationen ISACA German Chapter."

Wir stehen somit vor einer neuen Situation. Der Vorstand des ISACA Switzerland Chapters beschloss als Sofortmassnahme, die diesjährigen Ausgaben des ***NewsLetters*** von den für 2006 vorgesehenen fünf auf vier Ausgaben zu reduzieren. Für die Zukunft sind derzeit diverse Möglichkeiten in Diskussion. Anregungen nimmt Daniela Gschwend (Daniela_Gschwend@swissre.com) gerne entgegen.

Wir hoffen, die geschätzten Leser in der nächsten Nummer näher informieren zu können.

Das Redaktionsteam

D:

Aktivitäten des German Chapter

Am 10. März diesen Jahres haben wir unsere bisher größte Mitgliederversammlung des ISACA German Chapters in der seit Jahren bewährten Lokalität, dem Hilton Hotel in Frankfurt am Main, erlebt. Allein bei der Mitgliederversammlung haben 57 Mitglieder aktiv teilgenommen, insgesamt waren zusammen mit dem vormittäglichen Vortragsprogramm noch mehr Anwesende zu verzeichnen. Erstmals mussten wir daher den Raum ohne Tische für die Teilnehmer ausstatten, um allen Anwesenden einen Sitzplatz anbieten zu können. Diese Resonanz hat den Vorstand natürlich sehr gefreut, aber auch unter den Teilnehmern waren besonders rege Diskussionen zu sehen. Alle Themen und Entscheidungen können Sie dem bereits verschickten Protokoll zur Mitgliederversammlung entnehmen.

Ein Punkt, den ich hier gerne nochmals aufgreifen möchte, ist die Mitarbeit in Arbeitskreisen. Neben dem bereits sehr erfolgreich tätigen Arbeitskreis unter der Leitung von Herrn Neuy zum Thema Linux mit dem daraus entstanden Tool „Linux Audit Aid" gibt es aktuell zwei weitere neue Angebote:

1. Arbeitsgruppe zu CobiT/ITIL in Kooperation mit dem itSMF
Ansprechpartner: Herr Martini (Paul.Martini@itsmf.de) seitens des itSMF bzw. Herr Jürgen Gross (jgcons@aol.com) seitens des ISACA

2. Arbeitsgruppe zum Thema SAP
Ansprechpartner: Herr Christoph Triller (christophtriller@t-online.de) bzw. Herr Gunther Augustin (gunther.augustin@t-online.de)

Interessierten können wir nur raten: Nutzen Sie die Möglichkeit sich mit anderen Kollegen auszutauschen und eine lebhafte Arbeitsgruppe ins Leben zu rufen. Hierzu wenden Sie sich einfach an die o.g. Ansprechpartner, die Ihnen alles weitere zu der Arbeitsgruppe erzählen werden. Vielleicht werden dann auf der nächsten Mitgliederversammlung bereits erste Erfolge Ihrer Arbeitsgruppe bekannt gegeben.

Ingo Struckmeyer
Vorstand German Chapter

IT-Tagung 2006

In diesem Jahr findet zum zweiten Mal die IT-Tagung des IIR zusammen mit dem ISACA German Chapter in Deutschland statt. Nach dem Erfolg der ersten Veranstaltung im letzten Jahr haben die Veranstalter auch für dieses Jahr wieder einen aktuellen und interessanten Themenmix geschaffen.

Im Programm der IT-Tagung werden Vorträge insbesondere zu den aktuellen Themengebieten in der IT, die sich mit IT Governance sowie best practices in der IT beschäftigen, wie CobiT 4.0, ISO 20000 oder ITIL, aber auch klassische Prüfungsthemen wie SAP, Computer Forensics, individuelle Datenverarbeitung, Sicherheit oder Kontrollen im Unternehmen, angeboten. Das Ganze wird angereichert durch Diskussionsrunden zu einigen Themen und dem allgemeinen Austausch der Teilnehmer untereinander. Somit sollte für jeden von Ihnen etwas dabei sein, was bisher mit die-

ser Ausrichtung einmalig in Deutschland ist.

Sollten Sie Interesse an dieser Veranstaltung haben, dann schauen Sie einfach auf die Seiten isaca.de bzw. iir-ev.de und halten Sie sich den 22. bis 23. Mai 2006 für diese hochkarätige Veranstaltung in Frankfurt am Main frei. Wir freuen uns schon jetzt, Sie dort als Teilnehmer begrüßen zu dürfen.

Ingo Struckmeyer
Vorstand German Chapter

Referat von Herrn Willy Knüsel

CH:

Vereinsversammlung ISACA Switzerland Chapter

Am Donnerstag, 23. März 2006 fand in Biel die Vereinsversammlung 2006 statt. Willy Knüsel[1] beleuchtete in seinem Referat „E-Mail und Recht" das Tummelfeld von Meinungen, Behauptungen und Unsicherheiten. e-Mails befinden sich nicht in einem rechtsfreien Raum und deren Einsatz hat viele rechtliche Facetten. Näher ging der Referent auf den Vertragsabschluss vie e-Mail, die Aufbewahrungspflicht von e-Mails, den Datenschutz und SPAM ein. Rege genutzt wurde auch die Möglichkeit zur Diskussion und zum Austausch eigener Erfahrungen.[2]

Daniela S. Gschwend führte als Präsidentin souverän durch die Vereinsversammlung. Die Vorstandsmitglieder gaben einen Rückblick über die Tätigkeiten im 2005 und eine Vorschau auf 2006. Dauerthemen der Vorstandstätigkeit waren und sind die Ausbildung, Kommunikation und der ***NewsLetter***. Anerkennung fanden die reichen Vereinsaktivitäten in der Verleihung von je einem globalen und regionalen (Europa/Afrika) K. Wayne Snipes Chapter Recognition Award für 2004. Bruno Wiederkehr durfte die begehrten Auszeichnungen an der ISACA Leadership Conference 2005 im April 2005 in Las Vegas entgegennehmen.[3]

Ende 2005 zählte das Switzerland Chapter 685 Mitglieder; davon waren 326 CISA sowie 77 CISM. Sehr erfolgreich ist auch die Zusammenarbeit mit der Treuhand-Kammer, insbesondere die gemeinsam durchgeführten Kammer-Seminare zum Thema IT und die Übersetzung des Lehrmittels für die Akademie für Wirtschaftsprüfung. Trotz schwierigem wirtschaftlichem Umfeld konnten wir neun ISACA-Kurse durchführen und die After Hour Seminare fanden guten Anklang. Äusserst erfolgreich ist weiterhin der CISA-Kurs von Peter R. Bitterli, haben doch 96.4% der Kursteilnehmer 2005 die anspruchsvolle CISA-Prüfung bestanden. Ab 2006 können wir nun auch einen CISA-Kurs in der Westschweiz anbieten. Eine hervorragende Plattform für den Erfahrungsaustausch unter den Mitgliedern bilden auch die vielfältigen Interessengruppen.

Dank dem unermüdlichen Einsatz von Max F. Bretscher, Chefredaktor, und seinem Redaktionsteam haben wir mit dem ***NewsLetter*** einen sehr guten Stand erreicht. Leider aber wird das ISACA Germany Chapter ab Mitte 2006 nicht mehr mitmachen, sondern eine eigene Publikation herausgeben. Der Vorstand beschäftigt sich intensiv mit dieser Situation und ist auf der Suche nach einer geeigneten Lösung.

Breite Marketingaktivitäten helfen, ISACA, CobiT, CISA, CISM und IT Governance breit bekannt zu machen und deren Nutzen aufzuzeigen.

Genehmigt wurde auch die Jahresrechnung mit einem Verlust von CHF 400.31 (2004: Gewinn von CHF 14'326.34). Für 2006 ist ein Verlust von CHF 5000 veranschlagt, die Mitgliederbeiträge bleiben unverändert.

Für Studenten an Universitäten und Fachhochschulen vermitteln und betreuen wir Semester- und Diplomarbeiten und bieten neu bis zum 26. Altersjahr die Mitgliedschaft im ISACA Switzerland Chapter kostenlos an, sie bezahlen lediglich noch den internationalen Beitrag und haben so sehr günstig Zugang zum attraktiven ISACA-Angebot.

Neu in den Vorstand gewählt wurde Marc Barbezat, welcher sich vornehmlich um die Verankerung des Vereins in der Westschweiz kümmern wird. Die Präsidentin und der bisherige Vorstand wurden für 2006 wiedergewählt.

Rolf Merz

Endnoten

[1] Willy Knüsel, Knüsel Management AG, CH-4500 Solothurn; willy.knuesel@km-ag.ch www.mehrleisten.ch

[2] Das Referat wird publiziert auf www.isaca.ch

[3] NL Nr. 75/Juni 2005

ISACA AHS vom 31.01.2006 zum Thema: Value@IT bei E-Health, Kantonsspital St. Gallen

Am ersten After Hour Seminar (AHS) 2006 nahmen rund 20 ISACA Mitglieder teil. Das aktuelle Thema stand im Zeichen der von Bundesrat Deiss lancierten ePower-Initiative 2006. Aus dem Tagesanzeiger vom 19.01.2006 geht hervor, dass die Schweiz Punkto e-Government im EU-Vergleich auf den hintersten Plätzen rangiert. Der Bundesrat sieht im konsequenten Einsatz der Informations- und Kommunikations-Technologie (IKT) ein wichtiges Mittel, den Wohlstand in der Schweiz nachhaltig zu vermehren.

Der Referent, Herr Jürg Lindenmann, Leiter der Informatik des Kantonsspitals St. Gallen, hat aufgezeigt, dass der IKT-Nutzen von den meisten Partnern im Gesundheitswesen eingesehen wird. Es gelang dem Referent, die Nutzenpotentiale aufgrund der entwickelten e-Health Strategie aber auch die Stolpersteine klar aufzuzeigen. Die zukünftigen e-Health Möglichkeiten wurden den Mitgliedern anhand eines Videos plastisch dargestellt.

Als Hauptprobleme bei der Umsetzung wurden die folgenden Einflussfaktoren erwähnt:

- Hemmung durch die Politik der 26 Kantone „Kantönligeist“
- Fehlende gemeinsame Ziele/ Schwerpunkte (Spitäler, Ärzte „die Herren in weissen Mänteln“, Patienten „der gläserne Mensch“, Apotheken, Krankenkassen etc.)
- Mangelndes IKT-Verständnis (Professoren, Produzenten von medizinischen Geräten, Einsatz moderner IKT-Mittel, Infrastruktur etc.)
- Inkompatibilität hinsichtlich Informationsaustausch, -speicherung und -archivierung.

Aus dem Referat ging hervor, dass Standards und Mechanismen für Datenschutz und Datensicherheit vorhanden sind und für e-Health kein besonderes Problem darstellen.

Dass es aber bei der Umsetzung im Gesundheitswesen von besonderer Bedeutung ist, bekräftigte er mit dem Beispiel: Wenn im Rechnungswesen fünf Rappen falsch verbucht sind, ist es nur halb so schlimm. Wenn hingegen Informationen, wie Anamnese, Diagnose, Medikation falsch erfasst, vertauscht oder nicht verfügbar sind, kann dies schwere Folgen haben.

Interessante Fragen wurden dem Referenten zum Umbruch im Gesundheitswesen gestellt. Mit der äusserst kompetenten Beantwortung kamen die Mitglieder voll auf ihre Rechnung.

Fazit

Aus der Diskussion ging hervor, dass organisatorische und personelle Massnahmen notwendig sind sowie neue Herausforderungen an die Führungspersönlichkeiten im Gesundheitswesen gestellt werden müssen. Viele ausgabenwirksame Faktoren werden in den Spitälern heutzutage von Chefärzten bestimmt. Es stellt sich die Frage: Wer hat in der Medizin das Sagen? Unternehmerische Denkweise, modernes betriebswirtschaftliches Know-how, professionelle Kommunikation und Motivationsfähigkeit sind entscheidende Anforderungen, um einen optimalen IKT-Einsatz im e-Health zu gewährleisten.

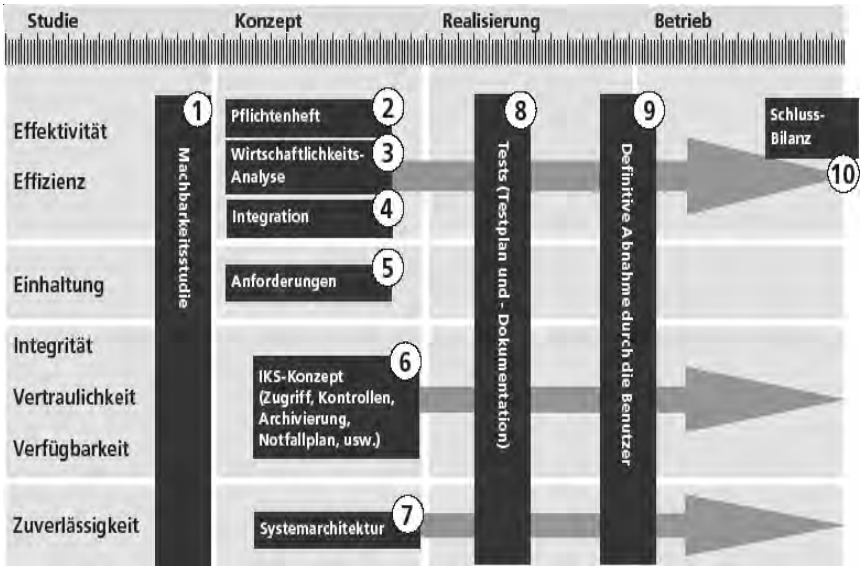


Abbildung: zehn Schlüsseldokumente für Informatikprojekte

Einmal mehr ist die Projektbegleitung und eben Value@IT durch die Revision gefragt. Sei es für die Unterstützung der Führungsfunktionen und des CIOs sowohl in Effizienz- und Effektivitäts-Fragen als auch in der Implementierung von adäquaten Kontrollen für die notwendige Informationssicherheit, Revisionsfähigkeit und Nachprüfbarkeit.

Als Hilfsmittel für den Gestaltungsprozess und die Projektbegleitung durch die Revision wurde auf die neuen Empfehlungen hingewiesen. Die zehn Schlüsseldokumente basierend auf dem CobiT-Referenzmodell können unter www.isaca.ch / Downloads / Arbeitsgruppen herunter geladen werden.

Bruno Wiederkehr

ISACA AHS vom 28.02.2006 zum Thema: Usability and Security

Im After Hour Seminar (AHS) vom 28. Februar haben uns zwei Experten aus ihrem jeweiligen Blickwinkel und Erfahrungsschatz die gegenseitigen Einflüsse von Software-Benutzbarkeit und IT-Sicherheit näher gebracht. Zu Beginn des AHS hat Herr H.R. Egli anhand von verschiedenen anschaulichen Beispielen eindrücklich aufgezeigt, wie häufig in der Informatik eine schlechte Benutzbarkeit direkt zu einer schlechteren IT-Sicherheit führt. Ob es schwer verständliche und schlecht handhabbare Verschlüsselungsprogramme, verwirrende Hinweis- oder Fehlertexte im Zusammenhang mit Zertifikaten oder schlicht unverständliche Systemmeldungen sind; der Benutzer ist in allen Fällen hoffnungslos überfordert und klickt nach dem Zufallsprinzip auf einen der verfügbaren „Buttons“. Häufig ist das die Ursache für einen weiteren, unnötigen Sicherheits-Zwischenfall. Ebenso problematisch sind Informatiklösungen, die an den Bedürfnissen der Benutzer vorbei entwickelt werden oder bei denen Sicherheitsaspekte nachträglich und unverständlich aufgepfropft werden. Dabei müsste doch eigentlich das Ziel der Software-Entwickler und Betreiber sein, Benutzbarkeit und Sicherheit so miteinander zu verschmelzen, dass Sicherheit sozusagen wie selbstverständlich (und für den Benutzer unmerklich) mitgeliefert wird.

Im zweiten Teil des AHS hat uns Herr Markus Flückiger vor Augen geführt, dass Sicherheit von Benutzern leider immer wieder als Hindernis empfunden wird; ob es nun um einfache Handhabung, Mobilität, Teamwork, Kompatibilität oder andere Aspekte geht. Um dies zu verhindern schlägt Markus Flückiger eine Reihe von Massnahmen vor, die eigentlich wie selbstverständlich im Software-Entwicklungszyklus eingebettet sein sollten.

Zuallererst muss akzeptiert werden, dass Sicherheitsanforderungen nicht am Ende einer Software-Entwicklung hinzugefügt werden können, sondern selber als funktionale Anforderung behandelt werden müssen. Sicherheitsfunktionen und -anforderungen müssen also konsequent in Use Cases modelliert werden, genau so wie alle funktionalen Anforderungen. Weiter zur angemessenen Integration von Sicherheit in eine Informatiklösung trägt eine sinnvolle Zusammensetzung des Projektteams bei. Begleitet werden muss ein Informatikprojekt durch einen Usability Engineer, einen Security Engineer und einen oder mehrere Benutzervertreter.

Die Schlussfolgerung aus dem Gehörten war für mich, dass Sicherheit nicht unabhängig vom Kontext entwickelt werden kann und genauso Aufgaben- bzw. Benutzerbezogen entwickelt und implementiert werden muss wie jede andere funktionale Anforderung.

Luc Pelfini

News aus den Interessengruppen

IG Operational IT-Risk

Peter R. Bitterli
Bitterli Consulting AG
Stampfenbachstr. 40
8006 Zürich
Tel. + 41 44 444 11 01
Fax. +41 44 444 11 02
prb@bitterli-consulting.ch

Die Interessensgruppe „Operational (IT) Risk“ hat sich neu formiert und entwickelt ein Konzept resp. Vorgehensvorschlag für ein „Risiko Management Kochbuch“. Ziel ist, Geschäftsleitungsmitgliedern, Führungsverantwortlichen im Business und der IT, Risikomanagement-Spezialisten und anderen Personen Schritt für Schritt aufzuzeigen, wie man für ein mittleres Unternehmen (eventuell auch für ein grosses Unternehmen mit wenig eigenen Informatiktätigkeiten) ein Risikomanagement aufbauen und erfolgreich beibehalten kann.

Derzeit werden keine neuen Mitglieder aufgenommen. Wenn die Ergebnisse vorliegen, wird die Interessengruppe darüber informieren.

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

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

Le groupe de travail qui rassemble les auditeurs informatiques des collectivités publiques a élaboré des recommandations à l'égard des responsables de projet informatique. Ce document d'une douzaine de pages est disponible en allemand, français et italien.

Les responsables de projet sont en effet soumis à de nombreuses contraintes et doivent conduire leurs projets au succès dans des conditions parfois difficiles. L'intervention d'un auditeur constitue un défi supplémentaire souvent perçu comme une inutile chicane par les responsables. Les Contrôles des finances estiment important de communiquer de manière ouverte et conséquente avec les responsables de projet. Cette brochure est là pour répondre à des questions qui sont fréquemment posées aux auditeurs. Elle contient également des informations intéressantes pour les décideurs, les responsables informatiques ou les personnes chargées de l'assurance-qualité.

L'objectif est notamment de déterminer la liste des documents les plus importants pour un auditeur et de définir les questions auxquelles ils doivent répondre. Cette brochure qui fait une large référence à CobiT se concentre sur la phase de projet qui constitue un passage important de la vie d'une application. Il existe en Suisse différentes méthodes de développement (y compris celles qui sont proposées par certains fournisseurs) et la terminologie peut varier de l'une à l'autre. Cette brochure se concentre sur le contenu des documents et fournit les références à ces différentes méthodes.

Ce document peut être téléchargé gratuitement aux adresses suivantes:
Deutsch : http://www.efk.admin.ch/pdf/novena_d.pdf
Français : http://www.efk.admin.ch/pdf/novena_f.pdf
Italien : http://www.efk.admin.ch/pdf/novena_i.pdf

Les membres de l'IG espèrent avoir grâce à cette brochure renforcé le dialogue entre les auditeurs et les responsables IT et contribué ainsi à un développement harmonieux et rentable des projets informatiques dans les administrations publiques suisses.

IG Computer Forensics

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

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

IG Einführung von IT-Governance

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

Letzte Sitzung: 24. Januar 2006 bei Bitterli Consulting AG in Zürich. Abnahme der Domäne „Beschaffung und Implementierung neuer Systeme". Besprechung Entwurf zur Domäne „Auslieferung und Unterstützung".

Nächste Sitzung: April/Mai 2006, Traktanden: Standortbestimmung der IG, Abnahme Domäne „Auslieferung und Unterstützung", Besprechung Entwurf zur Domäne „Plan und Organize".

IG Romandie

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

IG Outsourcing/Insourcing

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

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

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

IG MIS/EIS/DWH

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

Nach einer längeren Pause hat die IG ihre Arbeit wieder aufgenommen.

- Wrap-Up/Standortbestimmung

Es wurden alle bisher erstellten Dokumente aufgelistet und sofern sie noch finalisiert werden müssen, einem Verantwortlichen zur Bearbeitung zugeteilt.

- Weiteres Vorgehen

Das Referenzmodell und die Risiko-Matrix sollen als Resultat der Phase I (Datenextrakt und Load) nochmals überarbeitet und bereinigt werden. Danach sollen sie auf der Website der ISACA öffentlich zugänglich gemacht werden. Die diversen Fact-Sheets werden zum Teil nochmals überarbeitet zum Teil neu erstellt und gelten als Resultat der Phase II (Projektvorgehen und weitere relevante Aspekte).

- Wahl des neuen IG Leiters

Nach einer kurzen Besprechung ist der bisherige IG Leiter bestätigt worden. Es findet somit kein Wechsel statt.

- Diverses

Die Resultate sollen im Rahmen einer ISACA-Abendveranstaltung präsentiert werden.

Neue Interessenten können sich bei Daniel Oser, IG-Leiter, anmelden.

IG SAP R/3

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

Nächste Sitzung: 24. April 2006, 08:30 – 13:00, Bitterli Consulting AG, Zürich. Traktanden werden mit Einladung bekannt gegeben.

Monika Galli wird die Leitung der IG nach der Sitzung vom 24. April 2006 abgeben. Wir danken Monika für die langjährige und engagiert Führung der IG. Zusammen mit vielen Referenten hat sie uns interessante Aspekte der Prüfung im SAP R/3 Umfeld näher gebracht. Daher suchen wir einen neuen IG-Leiter. Interessenten melden sich bitte bei Monika Galli oder Rolf Merz.

IG (Self) Assessement mit CobiT 4.0

Leitung
Luc Pelfini, Bitterli Consulting AG
Tel: +41 44 444 11 00
prb@bitterli-consulting.ch

Diese IG konstituiert sich neu. An einer ersten Sitzung werden gemeinsam die Schwerpunkte und das Vorgehen definiert und verabschiedet. Ziel der IG ist die Erarbeitung eines Vorgehens und aller notwendigen Arbeitshilfen, um ein qualitativ hochstehendes (Self) Assessment basierend auf CobiT 4.0 durchführen zu können. Ein Schwerpunkt wird dabei sein, einen grössmöglichen Nutzen aus den neuen Bestandteilen von CobiT (z.B. RACI-Matrix) zu ziehen und die inhaltlich teilweise massiv überarbeiteten IT-Prozesse sowie deren Maturity Level für das (Self) Assessment zu verwenden. Grundsätzlich sollen aus CobiT 4.0 viele quantitative und qualitative Faktoren herausgeschält werden, so dass Assessment-Ergebnisse nachvollziehbar und objektiv sind. Die Arbeitsergebnisse werden voraussichtlich in MS-Office erstellt und sollen sowohl die Arbeit mit Papierexemplaren als auch die elektronische Erfassung und Auswertung der Assessment-Ergebnisse weitgehend unterstützen.

Datum der ersten IG-Sitzung: Montag, 29. Mai 2006, 17:00 – 19:00 Uhr. Stampfenbachstrasse 40 (Bitterli Consulting AG). Weitere Sitzungen im Raum Zürich, ausnahmsweise auch Bern oder Basel.

Traktanden der ersten IG-Sitzung mit Interessenten:

1. Vorstellung der potentiellen Mitglieder
2. Spielregeln der Arbeitsgruppe
3. Ziele und Prioritäten
4. Diskussion des Vorgehens und Definition erster Arbeitspakete
5. Konstituierung der IG

Mitglieder der IG (Self) Assessment mit CobiT 4.0: Angesprochen sind primär Personen, die bereits mit CobiT gearbeitet haben. Ebenfalls willkommen sind Personen, die CobiT nur kennen, aber nicht selber damit gearbeitet haben, sofern sich der Anteil der „Newcomer“ in angemessenem Rahmen hält.

Liebe IG-SAP'ler und Interessierte

Bald ist es wieder so weit. Unsere nächste Sitzung ist am

Montag, den 8. Mai 2006, (nicht am 24. April Sechseläuten!)
09.10 Uhr – ca. 12.30 Uhr
bei der ITACS Training AG, Stampfenbachstrasse 40, 8006 Zürich
Sitzungszimmer
ab Bahnhof SBB Tram 14 Richtung Oerlikon
Station Stampfenbachplatz (1. Halt) siehe auch beiliegender Plan

Die Traktanden sind:

1. Begrüssung
2. Sicherheitsstrategie SAP, am Beispiel des Kompetenzzentrums der Bundesverwaltung) was ist zu machen (und zu prüfen!)
   (Hr. Walter Bremer, Leiter Applikationsbetrieb CCSAP BV)
3. Tips und Tricks zur Prüfung im SAP FI (Hr. Roland Giger, Revisionsexperte EFK)
4. Erfahrungen und News (alle)
5. Diverses
6. Abschluss spätestens 13.00 Uhr (Raum wird anschliessend gebraucht)

Wir können sicher irgendwo gemeinsam Mittagessen, wenn dies gewünscht wird.

Es wäre schön, wenn Sie auch dieses Mal recht zahlreich erscheinen würden. Ich werde nächstes Jahr nach 47 Jahren Berufsarbeit in meinen wohlverdienten Ruhestand treten und gebe deshalb die Leitung der IG SAP ab.

Das Protokoll und die Unterlagen der letzten IG vom Nov 2005 werde ich Ihnen in den nächsten Tagen zukommen lassen. Ich freue mich, Sie bald begrüssen zu dürfen.

Freundliche Grüsse

M. Galli

M.E. Galli (CISA, CISM)
Eidg. Finanzkontrolle
Fachbereich 2
Monbijoustrasse 45
CH-3003 Bern

Tel. +41 31 324 94 95
Fax +41 31 323 11 01
E-Mail: monika.galli@efk.admin.ch
WEB: www.efk.admin.ch

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Veranstaltungen

CISA-Prüfungsvorbereitungskurs	3. April–15. Mai 2006 Zürich, 5 Tage, ISACA/ITACS
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	19.–21. April 2006 Zürich, 3 Tage, ISACA/Compass
After Hour Seminar: Mit der Brille der Ethik (Umgang mit Konflikten in der Arbeit von (Informatik)-Revisoren	25. April 2006 16.40-17.40, Zürich, ISACA
Evidence Lab – Workshop über die Spurensuche in Computersystemen	26.–28. April 2006 Zürich, 3 Tage, ISACA/Compass
Préparation à la certification internationale CISA	1 mai au 8 juin 2006 Lausanne, 18 soirées, ISACA
Content und Mobile Security Lab	3.–5. Mai 2006 Zürich, 3 Tage, ISACA/Compass
BS7799/ISO27001 Zertifizierter Lead Auditor	8.–12. Mai 2006 Zug, 5 Tage, Infoguard
SSI-Fachtagung Existenzsicherung im Krisenfall	10. Mai 2006 Zürich, 1 Tag, Mediasec
Anwendungssicherheit: Risiko-orientierte Entwicklungsmethoden	22.–24. Mai 2006 Zürich, 3 Tage, ISACA/ITACS
IRR-Tagung	23. Mai 2006 Frankfurt, 1 Tag, ISACA Germany
Hacker, Spione und Datendiebe	29.–31. Mai 2006 Zug, 3 Tage, Infoguard
Intensivlehrgang SIBE	29. Mai – 2. Juni 2006 Zürich, 5 Tage, Infosec
After Hour Seminar: Thema noch nicht bekannt	30. Mai 2006 16.40–17.40, Zürich, ISACA
SSI-Fachtagung: Synergien im baulichen und technischen Schutz	31. Mai 2006 Zürich, 1 Tag, Mediasec
Content- und Mobile-Security Lab – Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Tech. und aktuelle Malware	3.–5. Juni 2006 Zürich, 3 Tage, ISACA/Compass
Service Management – ITIL Foundation Training – Auf der Basis des de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	7.–9. Juni 2006 Zürich, 3 Tage, ISACA/Glenfis
BS 15000 Consultant & Internal Auditor, inkl. int. Zertifizierung	12.–14. Juni 2006 Zürich, 3 Tage, ISACA/Glenfis
The 3rd Annual CISO ExecutiveSummit & Roundtable, Barcelona	14.–16. Juni 2006 Barcelona, 3 Tage, MIS
Anwendungssicherheit: Risikoorientierte Entwicklungsmethoden	22.–24. Juni 2006 Zürich, 3 Tage, ISACA/ITACS

Kontaktadressen Veranstalter

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

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

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

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

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

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

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

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

ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel. + 41 44 444 11 01
Fax +41 44 444 11 02
info@isaca.ch
www.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

ITACS Training AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel. +41 44 444 11 01
Fax +41 44 444 11 02
info@itacs.ch
www.itacs.ch

Management Circle
Hauptstrasse 129
D-65760 Eschborn/Ts.
Tel. +49 6196 4722-800
anmeldung@managementcircle.de

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

Serview GmbH
The Business IT Alignment Company
Gartenstrasse 23
D-61352 Bad Homburg
Tel. +49 6172 177 44-0

Swiss Infosec AG
Weissensteinstrasse 2b
CH-3008 Bern
Tel. +41 31 300 73 73
Fax +41 31 300 73 78
infosec@infosec.ch

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

Vereon AG
Rosgartenstrasse 37
CH-8280 Kreuzlingen
Tel. +41 71 670 19 14
Fax. +41 71 670 19 13
info@vereon.ch
www.vereon.ch

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

Vereinsadressen

Germany Chapter

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

Präsidentin
Karin Thelemann
Tel. +49 6196 99626 488
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Tel. +49 69 9587 2313
MGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
Tel. +49 201 438 0
Norbert.Groening@de.pwcglobal.com

Public Relations
Heinrich Geis
Tel. +49 692 101 5149
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
Tel. +49 4106 704 2336
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Holger Klindtworth
Tel. +49 (40)41522863
h.klindtworth@susat.de

www.isaca.de

Austria Chapter

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand
Tel: +43 1 31332 656
m.schirmbrand@kpmg.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Tel: +43 1 53127 2857
maria-theresia.stadler@oekb.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner
PricewaterhouseCoopers
Tel: +43 1 501 88 1701
josef.renner@at.pwcglobal.com

Schriftführer, Mitgliederversammlung, Marketing
Mag. Gunther W. Reimoser
Tel: +43 1 12 111 701 032
gunther.reimoser@at.ey.com

Kassier, Webmaster
Mag. Jimmy Heschl
Tel: +43 1 31332 619
jimmy@heschl.at

CISA/CISM-Koordinator
Mag. Ulrike Knödlstorfer-Ross
Tel: +43 1 33151 145
ulrike.knoedelstorfer@ama.gv.at

NewsLetter-Koordination
Mag. Dieter Stangl-Krieger
Tel: +43 1 31332 619
DStangl-Krieger@kpmg.at

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

www.isaca.at

Switzerland Chapter

Präsidentin
Daniela S. Gschwend
Tel. +41 43 285 69 36
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Tel. +41 31 323 10 35
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Tel. +41 71 626 64 61
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Tel. +41 44 444 11 00
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Tel. +41 44 421 64 22
tbucher@deloitte.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Tel. +41 61 324 09 59
monika.josi@novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Tel. +41 58 286 66 79
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Marc Barbezat
Tel. +41 x
paul.wang@

Marketing
Bruno Wiederkehr
Tel. +41 44 910 96 33
bru.wiederkehr@bluewin.ch

www.isaca.ch