IT security & data protection - the benefit of integration

Two complementary sides of the same story

Kerstin Blossey[1], Markus Väth[2]

KSB4 Consulting - Geschäftsleitung

[1]kblossey@ksb4.net

KSB4 Consulting - Bereich Datenschutz, Personalentwicklung

[2]mvaeth@ksb4.net

Abstract

Aktuelle Trendumfragen zeigen, dass sich der Schwerpunkt in der IT von technischen Aspekten auf ein ganzheitliches Daten- und Informations-Sicherheitsmanagement verlagern wird. Informationstechnische Vorkehrungen werden im Systemumfeld um den Faktor „Mensch“ zu erweitern sein. Die IT allein kann dies nicht leisten, da schon die erforderliche fachliche Spezialisierung professioneller IT-Kräfte ganzheitlich orientierte Kompetenz logisch ausschließt. Darüber ist der Spagat zwischen klassischen IT-Maßgaben - die Vorhaltung möglichst umfangreicher Datendepots mit einer möglichst vielfältigen Applikationspalette - einerseits und dem Anspruch nach einem maßvollen Daten- und Informationsmanagement zum Schutz des Unternehmens bzw. zum Schutz personenbezogener Daten, generell nicht zu empfehlen, da kontraproduktiv.

Datenschutz im Unternehmen sollte daher nach dem Gesetz personell nicht vom Management oder der IT-Leitung betrieben werden, ebenso wenig wie von einem Volljuristen ohne jeglichen technischen Horizont. Spätestens seit Ende Mai 2005 verstoßen alle Stellen, welche Personendaten automatisiert nicht rein privat verarbeiten, gegen geltendes EU- und nationales Recht. Dabei handelt es sich keineswegs um ein Kavaliersdelikt in juristischen Grauzonen, Unwissenheit schützt auch hier vor Strafe nicht. Im Haftungsfall sieht das Bundesdatenschutzgesetz Bußgelder von bis 250.000 Euro bzw. Haftstrafen von bis zu zwei Jahren vor.

In Zeiten standardisierten Qualitätsmanagements, als „nice to have“ für eine wohlwollende Bonitätsbewertung und als Wettbewerbsargument gegenüber potentiellen Geschäftspartnern, zeugt es nicht nur von verwunderlicher Resistenz gegenüber der Gesetzgebung, sondern vor allem von wirtschaftsökonomischer Kurzsicht. Die kooperative Zusammenarbeit von Datenschutz und IT-Sicherheit schaffen Transparenz und praktizierbare Optimierung der Geschäftsprozesse, Sensibilisierung des Personals für den Wert von Daten und Informationen und beugen so wirksam vielen Ansätzen der Wirtschaftsspionage vor und sorgen so für den Schutz personenbezogener und unternehmenssensibler Daten sowie für eine gesetzlich verordnete Qualitätssicherung durch eine zusätzliche analytisch-unabhängig Instanz im Unternehmen.

Index

All necessary clearances for the publication of this paper have been obtained. If accepted, the author will prepare the final manuscript in time for inclusion in the conference proceedings and will present the paper at the conference.

1 Datensicherheit als Bestandteil der IT - Tasks

Datenverarbeitung ist aus der heutigen Wirtschaft, ob Global Player oder KMU, nicht mehr wegzudenken. Eine gut strukturierte IT ist das Rückgrat jedes modernen Unternehmens. Eine genau auf das Unternehmen zugeschnittene hochleistungsfähige Server-Architektur oder die Sicherheit auf allen elektronischen Kommunikationswegen, sei es E-Mail, Messenger, Videokonferenz-Systeme oder eine der vielfältigen anderen Möglichkeiten – die interne IT-Infrastruktur steht im Mittelpunkt des Geschehens bei der technischen Umsetzung von Kernerfordernissen.
Diese Kernerfordernisse zeichnen sich durch eine sukzessive Komplexität aus, unabhängig davon, ob es um die Konfiguration unterschiedlicher Hard- und Software geht, um die Gestaltung und Umsetzung von Policies zum verantwortlichen Umgang mit Daten im Geschäftsprozess bis hin zum internen und externen Support und grenzüberschreitenden Datenströmen, die mittels weniger Mouseklicks und wenig Nachdenken über den Grenzübertritt im „global village“ längst geographische Entfernungen und Kulturunterschiede tagtäglich mühelos überwinden.

1.1 Neues Rollenverständnis

Neueste Umfragen prophezeien bereits seit Anfang des Jahres die Verschiebung der traditionellen Rolle des CIO und der IT im Unternehmen. Den „IT-Trends 2007“ von Capgemini (3) folgend, wird sich die IT vermehrt mit geschäftsprozess-beratenden Aufgaben anfreunden müssen, insbesondere in Firmen, die ihre klassische IT-Bereiche auslagern wollen oder dies bereits in den letzten zwei Jahren getan haben. Dabei bleiben die klassischen IT-Aufgaben bestehen.

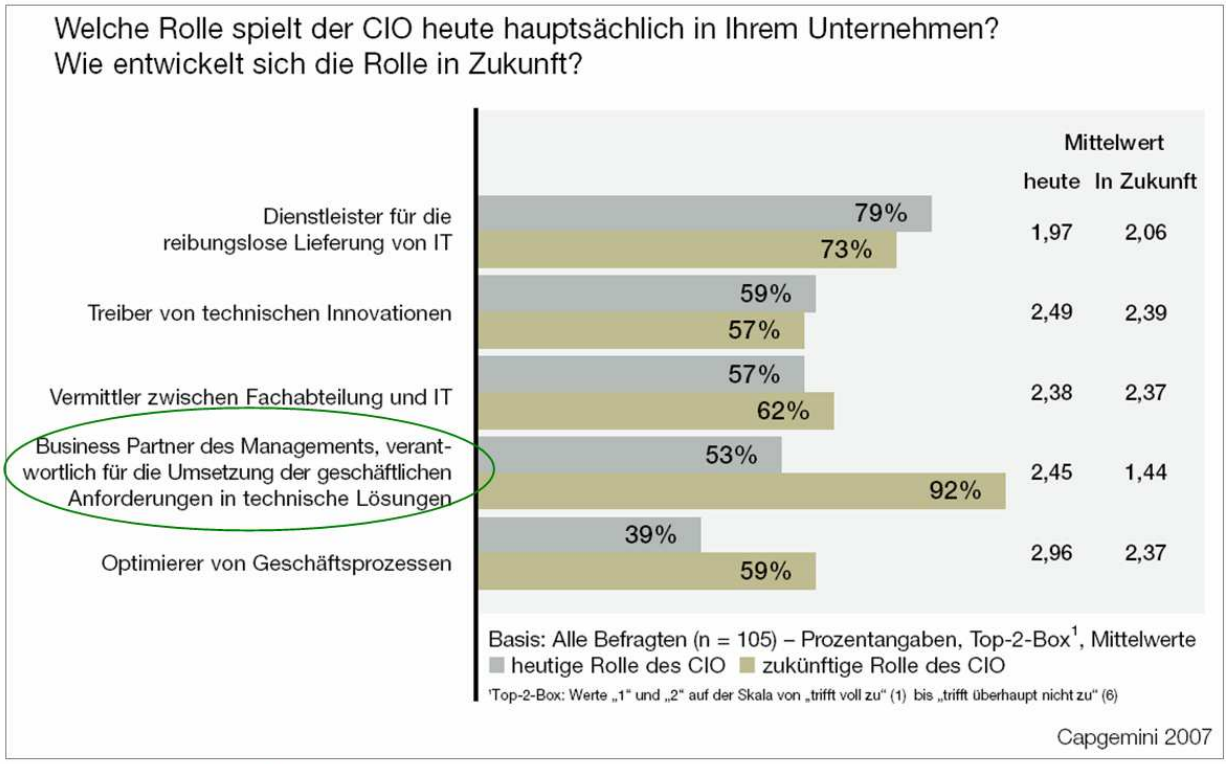

Abbildung 1: Verlagerung der Rolle der CIO

Interdisziplinäres Schnittstellenmanagement zur Vermittlung zwischen Fachabteilungen, hierarchischen Unternehmensebenen und der IT sowie die Optimierung von Geschäftsprozessen werden laut Abbildung 1 das Aufgabenfeld des IT-Administrators ebenso ergänzen wie das des CIO. Mit steigender Komplexität der Funktion des IT-Administrators nimmt naturgemäß auch der Anteil an erforderlichen Sicherheitsmaßnahmen außerhalb des technischen Kernbereichs zu. In diesem Bewusstsein werden die IT-Abteilungen - und damit der Bereich der Datensicherheit - zu einem integralen Bestandteil der Unternehmensführung.

1.2 Verlagerung der Sicherheitsrisiken

Obwohl es je nach persönlicher Philosophie unterschiedliche Ausprägungen insbesondere der CIO–Tätigkeit gibt, sollte neben der visionären Komponente („Wo streben wir hin?“) auch eine beachtliche Wissenskomponente („Wo kommen wir her?“) und eine stetige Wachsamkeit gegenüber den Bedrohungen der modernen vernetzten Gesellschaft stehen („Wie machen wir den Laden sicher?“). Applikationen kann man wieder aufspielen, Hardware ersetzen, doch versehentlicher sowie (von innen oder außen) provozierter Datenverlust ist nicht so leicht, und in vielen Fällen überhaupt nicht, kompensierbar. Die IT–Sicherheit spielt eine immens wichtige Rolle dabei, das rasant wachsende und ständig mutierende Feld potentieller Angriffe im Blick zu behalten. Waren bisher Begriffe wie Viren, Würmer und Spam-Überflutung in aller Munde, gilt es heute, echtem (und leider größtenteils automatisiertem) Cracking, wie Phishing, Pharming etc., und dem Reverse Engineering zu begegnen.

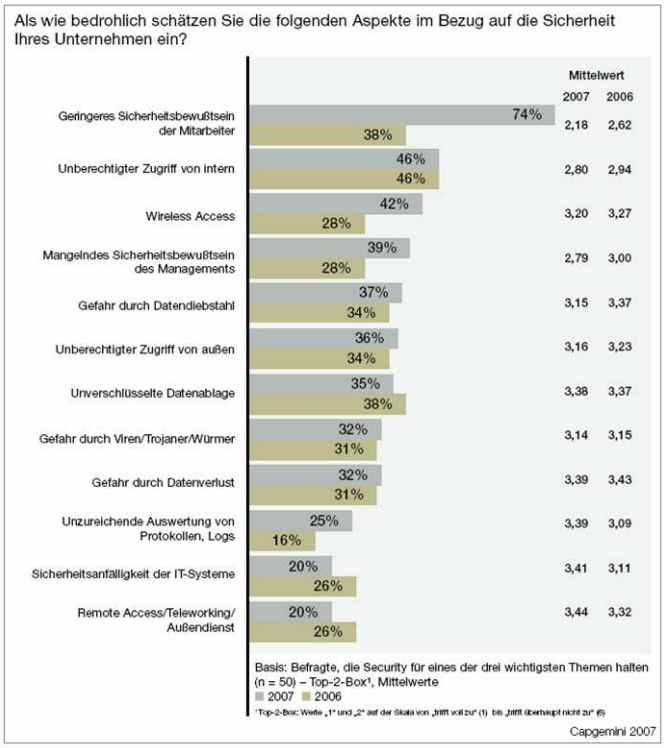

Abbildung 2: Risikofaktoren im Bezug auf die IT-Sicherheit im Unternehmen

Hinzu kommt der seit „Mitnick“ verstärkt ins Fachvokabular aufgenommene „Risikofaktor Mensch“ (13), bei dem nicht mehr allein die technische Abwehr zählt, sondern vor allem die Begegnung auf der sozialen Ebene. Technische Maßnahmen sind in mittelständischen Unternehmen in der Regel etabliert, was sich unter anderem in der Budgetierung widerspiegelt. Jedoch Sicherheitslücken in Form des Umgangs mit mobilen Datenträgern wie Laptops im Außendienst, Blackberries und Handhelds im Management und die allgegenwärtigen USB-Speichersticks, die künftig vermehrt von handlichen externen 2,5“-Festplatten abgelöst werden, haben selbst namhafte internationale Konzerne oft erschreckend wenig entgegen zu setzen.

Ein Grund dafür ist die mangelnde Sensibilität des Personalstabs im Bezug auf den Wert digitaler Daten und Informationen. „Wie sorgsam stellt Ihre Firma sicher, dass vertrauliche Daten nicht dort abgelegt werden, wo sie gerade für das Publikum zugänglich sind, vor dem Sie es eigentlich schützen wollen?“, fragt Kevin Mitnick (13), einer der wohl bekanntesten Hacker, der

heute ein erfolgreicher IT-Sicherheitsberater ist. Interessant am Umfrageergebnis der Capgemini-Studie (siehe Abbildung 2) ist, dass auf den ersten vier Plätzen nicht die Technik, sondern der „Unsicherheitsfaktor Mensch“ im Mittelpunkt steht. „Geringes Sicherheitsbewusstsein der Mitarbeiter (74%), „Unberechtigter Zugriff von intern“ (46%) sowie „Mangelndes Sicherheitsbewusstsein des Managements“ (39%) sind nach Meinung der befragten CIOs mit die wichtigsten Herausforderungen. Und die Frage, die oben als Zitat genannt wird, hat längst konkrete Vorfälle in der Praxis erhalten: Anfang 2007 ging durch die Presse, dass die Ergebnisse einer polizeilichen Verkehrskontrolle auf einer deutschen Bundesautobahn irrtümlich statt im behördlichen Intranet im öffentlich zugänglichen Internet eingestellt wurden – und so Personalien von Autofahrern inklusive aller Alkohol- und Drogentestergebnisse und verhängter Sanktionen für alle vernetzten findigen Internetnutzern einsehbar waren (15).

Zusätzlich können Sicherheitslücken im Unternehmen auch ohne jeglichen Einsatz von IT eklatant werden. Geraten sie ins Licht der Öffentlichkeit, ist ein Imageverlust kaum zu verhindern – von Schadensersatz oder gar einem Strafmaß nach StGB ganz zu schweigen. Auch hier gibt es eine ganze Reihe von Beispielen, und sie alle verdeutlichen in erschreckendem Maß die dringende Notwendigkeit einer Sensibilisierung des Personalstabs. Zwei seien stellvertretend genannt: Spielende Kinder finden auf offener Straße entsorgte Patientenakten aus einer Arztpraxis neben einem Papierkontainer (10); ein großer Mobilfunk-Anbieter in Griechenland muss auf Veranlassung der verantwortlichen Datenschutzbehörde 76 Millionen Euro für seine Verwicklungen in einen Abhörskandal bezahlen (12).

1.3 Interessengruppen und ihre Anforderungen an die IT

Die interne IT steht also im Spannungsfeld zwischen Sicherheit der computergestützten Systeme und der Sicherheit rund um diese Systeme herum. Zusätzlich stehen sie zwischen unterschiedlichen Interessensgruppen und deren jeweilige Einflussnahme: Mitarbeiter, Geschäftsleitung, Kunden, Partner, Gesetzgeber. Nicht nur informationstechnische, sondern auch politische, kommunikative, gesellschaftliche und juristische Anforderungen sind von den CIOs und ihren Administratoren gestellt, mit denen sie sich zunehmend arrangieren müssen (s. Abbildung 3).

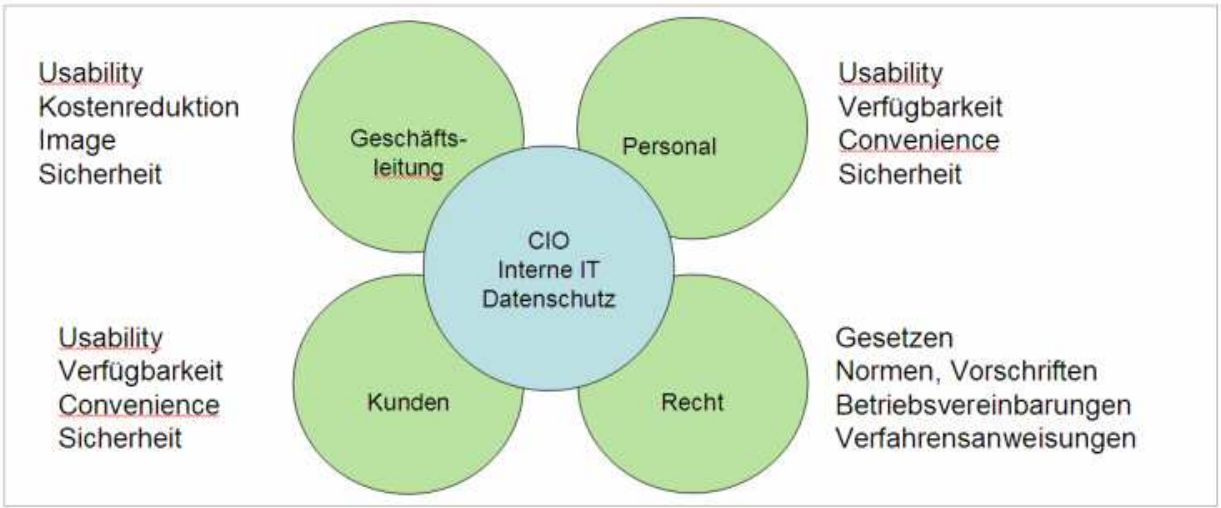

Abbildung 3: Interessensgruppen und ihre Anforderungen

Die IT und damit ihr CIO kämpfen daher an mehreren Fronten: Einmal müssen sie möglicherweise unbeliebte Sicherheitsmechanismen installieren bzw. implementieren, wobei sie auf Widerstand der Geschäftsleitung und der Mitarbeiter stoßen. Hier findet sich der Widerspruch zwischen Usability und Sicherheit, zwischen Convenience und Spionageabwehr. Auf der anderen Seite soll die IT auf Erfordernisse eingehen, die berechtigt von außen an sie herangetragen werden. Hierzu gehören beispielsweise der Bereich des geltenden Rechts und damit zum Beispiel der Datenschutz oder das Qualitätsmanagement. Im Gegensatz zu althergebrachten, technisch orientierten Aufgaben „[...] scheint die zukünftige Aufgabe noch nicht definiert zu sein. Die bereits bekannten Anforderungen werden um neue erweitert: Die Prozesse müssen optimiert, die Wirtschaftlichkeit berechnet und das Geschäft vorangebracht werden. Dazwischen bleibt wenig Zeit, sich über Strategien Gedanken zu machen [...]“ (3). Das Ergebnis jeglicher Business Intelligence muss folglich lauten: eine praktikable Lösung muss her, und zwar eine, die mit einem hybriden Riskmanagement fertig wird ohne die ERP-Harmonisierung zu stören, einhergehend mit einem Paradigmenwechsel – eine Folgerung, die Capgemini bereits in seiner Trendumfrage 2005 formuliert hat (4).

2 Datenschutz als Bestandteil der IT-Sicherheit

Bei allen bisher genannten Vorfällen und bei dem Spagat zwischen IT-Administration und allgemeinem Informationssicherheitsmanagement, dem CIO und seine IT künftig verstärkt ausgesetzt sein werden, kann ein professioneller Datenschutzbeauftragter entscheidende Schützenhilfe leisten und nachhaltigen Schaden vermeiden helfen.

2.1 Hintergrund zum Datenschutz

Datenschutz ist in Deutschland spätestens seit Mai 2001 gesetzliche Anforderung an jedes Unternehmen, in denen eine definierte Anzahl Mitarbeiter "personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen" (§ 4f BDSG) - eine Tatsache, die eine erschreckende Mehrheit der Firmen, Verbände, Vereine und sogar vieler Behörden offenbar nicht bewusst oder unwichtig ist. Außer Acht gelassen wird hierbei der Umstand, dass bereits bei fehlender Bestellung eines Datenschutzbeauftragten ein Bußgeld von bis zu € 25.000 und bei einem Verstoß gegen Datenschutzbestimmungen sogar das Zehnfache, eine Geldstrafe bis zu € 250.000 oder gar eine Haftstrafe verhängt werden kann (§§ 43, 44 BDSG). Wie teuer ein Vorfall in der Praxis kommen kann, wen es zu konkreten Datenschutzvorfälle kommt, zeigen zwei an dieser Stelle zeitlich etwas zurückliegende, aber in den Köpfen präsente Fälle: Ein großer deutscher Versicherungsunternehmen, bei dem die Einsichtnahme in Versichertendaten von mehr als 2.500 Kunden über das Internet möglich war (11) und die „Kranich-Affaire“ um das Bonusmeilen-System einer bekannte Fluggesellschaft, die einen so massiven Imageschaden verursachte, dass sie den Rücktritt namhafter Politiker zur Konsequenz hatte (6).

In Deutschland gründen sich die Datenschutzbestimmung (9) auf das Bundesdatenschutzgesetz (BDSG), die nationale Umsetzung der EU-Richtlinie (7). Bereits in den frühen Achtzigern erkannte der Gesetzgeber, dass der Umgang mit personenbezogenen Daten einer Regulierung bedürfe. „Personenbezogene Daten“ umfassen dabei „Einzelangaben über eine bestimmte oder bestimmbare Person“ (§ 3 BDSG). Dies können Daten über persönliche Verhältnisse (Name, Geburtsdatum etc.) oder sachliche Verhältnisse (Steuer, Kfz-Typ, Versicherungen, Arztdaten etc.) sein. Das BDSG bildet die gesetzliche Grundlage für die automatisierte Verarbeitung sol-

cher Daten und belegt diese mit einem generellen Bearbeitungsverbot. Dieses Verbot kann lediglich durch begründete Ausnahmen, die im Gesetz dargelegt sind, aufgehoben werden. Über die Rechtmäßigkeit einer automatisierten Datenverarbeitung zu entscheiden und den Umgang mit personenbezogenen Daten gesetzeskonform zu regeln, liegt in der beratenden Verantwortung des fachkundigen Datenschutzbeauftragten, der als Funktion outgesourced werden kann.

2.2 Aufgaben des Datenschutzes

Rolle, Funktionen und Aufgaben des Datenschutzbeauftragten sind im Bundesdatenschutzgesetz festgelegt und umschrieben, vor allem geht es dabei um:

- Überwachungspflicht (§ 4g Abs. 1 Nr. 1 BDSG)
- Vorabkontrolle (§ 4d Abs. 5 BDSG)
- Personal-Sensibilisierung (§ 4 g Abs. 1 Nr. 2 BDSG)
- Öffentliches Verfahrensverzeichnis (§ 4g Abs. 2 BDSG)
- Durchführung ggf. erforderlicher Meldungen gegenüber der Behörde (§ 4 d BDSG)
- Pflege des internen Verfahrensverzeichnisses und interner Richtlinien (§ 4 e BDSG)
- Verpflichtung des Personalstabs auf das Datengeheimnis (§ 5 BDSG)
- Beratung zu technisch-organisatorischen Maßnahmen (§ 9 BDSG und Anlage)
- Überprüfung externer Dienstleister auf Datenschutz-Erfordernisse (§ 11 BDSG)
- Datenschutz-Audits (bzw. Audits durch externe Dienstleister, § 9 a BDSG)
- Auskunftsersuchen von Betroffenen (§ 6 BDSG)
- Grenzüberschreitender Datenschutz (§ 4 b BDSG)
- Aufbau einer internen Datenschutzorganisation (§ 4g Abs. 2 BDSG)
- Berichterstattung an die Geschäftsführung (§ 4g Abs. 2 BDSG)
- Beratung und Mitwirkung, z.B. bei der Gestaltung von Formularen und Verträgen
- Vertretung des Unternehmens nach außen (Betroffene, Behörden etc.)

2.3 Vorteile des Datenschutzmanagements für das Unternehmen

Die Arbeit des Datenschutzbeauftragten und seine Installation im Unternehmen mit dem juristischen Hintergrund des BDSG haben für das Unternehmen als Ganzes einige Vorteile, die sich nicht nur rechtlich sondern auch monetär auszahlen:

1. Rechtssicherheit. Es wird kontinuierlich daraufhingearbeitet, dass IT-Vorgänge nicht gegen geltendes Recht verstoßen. Beispiel: Pflege der Kundendatenbank nach den Anforderungen Datensparsamkeit und Beachtung von Löschungsfristen.
2. Imagegewinn. Ein Unternehmen gewinnt an Ansehen, wenn es sich durch ein modernes, mitarbeiter- und kundenorientiertes Verhalten im Umgang mit sensiblen Daten auszeichnet.
3. Kostenreduzierung durch Prozessoptimierung. Die Datenschutzanalyse der Prozesse im Unternehmen schafft oft eine neue Transparenz, die noch nicht genutzte Synergien aufzeigt. Stichwort: „Die linke Hand weiß nicht, was die rechte tut.“ Ein extern bestellter Datenschutzbeauftragter kann analytisch wirksamer handeln, da er gegenüber den Gepflogenheiten im Unternehmen noch objektiv gegenübersteht (Betriebsblindheit).
4. Schutz der Mitarbeiter. Durch Datenschutz wird sichergestellt, dass keine unzulässigen Leistungskontrollen vorgenommen werden, durch klare Datennutzer-Konzepte werden die Risiken des Mobbing und anderer sozial-kritischer Aspekte verkleinert.

5. Rechtliche Entlastung. Die Mitarbeiter, und in der Konsequenz die Geschäftsleitung, stehen in der Gefahr, für Fehler bei der automatisierten Datenverarbeitung haftbar gemacht zu werden. Zumindest für den Bereich des Datenschutzes kann dieses Risiko eine professionelle Datenschutzorganisation wirksam reduziert werden. Im Sinne des Unternehmens nimmt der Datenschutzbeauftragte in der Unternehmenshierarchie eine Stabsstelle ein und wahrt seine fachliche Unabhängigkeit durch ein direktes Vortragsrecht bei der Geschäftsleitung und sowohl weisungsfrei als auch ohne Weisungsbefugnis operiert.

Datenschutz und Datensicherheit sind reale Aufgabenbereiche im Unternehmen, deren Vernachlässigung einschneidende Folgen haben können. Die bisher genannten Praxisbeispiele bieten im Wissenstransfer vielfach Lösungsansätze.

Während der Trend zum Outsourcing der IT derzeit eine organisatorische Vollbremsung durch vielfältige Umsetzungshindernisse erfährt, empfiehlt sich bei der Realisierung des Datenschutzes im Unternehmen geradezu eine Auslagerung an einen kompetenten externen Dienstleister. Folgende Vorteile biete eine externe Datenschutzdienstleistung:

→ **Stellung im Unternehmen**
- Unabhängig im Sinne des BDSG, weisungsfrei
- Unterliegt weder Betriebsrat noch anderen Organen
- Problemlosere Kündbarkeit
- Regressmöglichkeit

→ **Optimale Qualifikation**
- Intensive Fortbildungsmöglichkeiten
- Kontinuierliche Weiterbildung
- Gute Kontakte zu wichtigen Anlaufstellen

→ **Zuverlässigkeit**
- „Nicht betriebsblind“
- Effektiver Ressourceneinsatz
- Professionelles Datenschutz-Management
- Ungeteilte Datenschutz-Aufmerksamkeit

→ **Außenwirkung**
- Bearbeitung von Stellungnahmen etc.
- Repräsentant für Anfragen von außen und innen
- Datenschutz als Image- und Wettbewerbsvorteil

Abbildung 4: Vorteile eines externen Datenschutzbeauftragten im Unternehmen

Die Einbeziehung eines externen fachkundigen Datenschutzbeauftragten in den Betrieb macht das Abziehen anderweitig hoch qualifizierten Personals unnötig und bringt frischen Wind von außerhalb. Darüber hinaus profitiert das Unternehmen von einem ständigen Austausch des externen Dienstleisters in Fachkreisen und mit Kollegen, da dieser von tagesaktueller best practice abhängig ist in seiner Leistungsqualität.

3 Ziele und Synergien

IT-Sicherheit und Datenschutz sind wichtige Bereiche in zeitgemäß geführten Unternehmen, die sich in der Praxis hervorragend ergänzen: der technisch geprägte Fokus der IT und der ganzheitlich-interdisziplinäre Ansatz professionellen Datenschutzes sichern sowohl gesetzliche als auch wirtschaftökonomische Anforderungen im Unternehmen. Beide Aspekte sind die zwei Seiten einer weithin geläufigen Medaille namens Betriebssicherheit mit ähnlichen Zielen.

3.1 Synergie zweier operativer Ebenen

IT-Systeme aller Art - vom analogen Standalone-Faxgerät über die veraltete Bandmaschine bis hin zum Hightec-Computersystem mit optischer Verkabelung und Satelliten-Anbindung in alle Welt sowie alle nur denkbaren Informations- und Rechnerfarmen - haben eines gemeinsam: Sie haben im Grunde mit denselben Risikofaktoren und Gegnern zu kämpfen, wie wir, der seit Mitnicks Veröffentlichungen gegenständlich benannte „Faktor Mensch“. Die Risikofaktoren sind im Cyberspace kaum andere als in der Virtual Reality, das beweisen unzählige deutsche und internationale Studien und Umfragen der letzten Jahre. Diese Risikofaktoren lassen sich hervorragend mit folgender Grafik der ASK IT-Secure GmbH (1) auf den Punkt bringen:

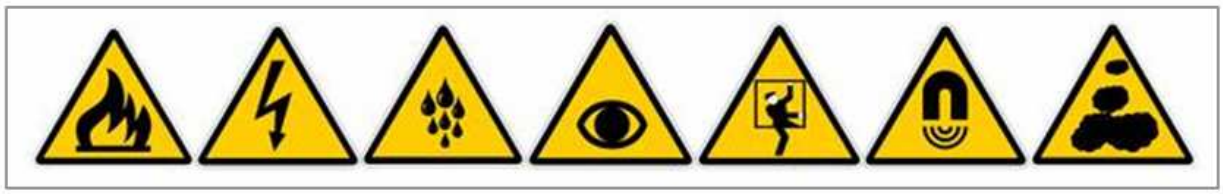

Abbildung 4: IT-Risikofaktoren im Unternehmen

Administratoren kämpfen gegen Umwelt- und Umgebungseinflüsse, die sich gut in die drei Kategorien „Naturkatastrophen“, „Materialschwächen“ und „menschliches Versagen“ klassifizieren lassen. Der professionell betriebene Datenschutz wirkt in denselben Kategorien. Dabei führen IT-Administration und betrieblicher Datenschutz diesen Kampf auf zwei Ebenen: auf der technischen Ebene des IT- oder des automatisierten Systems, zum anderen auf der sozialen Ebene der IT-Peripherie oder der Ebene des Anwenders und seinem Kontext. Das Ziel ist, die Infrastruktur an sich so sicher wie möglich (IT) bzw. so angemessen sicher wie möglich (Datenschutz) zu gestalten und parallel den Fall des „DAU“, des „dümmsten anzunehmenden Users“, also des Menschen, der die Technik bedienen soll, zu vermeiden.
Datenschutz und IT-Administration stehen auf derselben Seite. Auch die Anforderungen, die an IT-Systeme und automatisierte Verfahren gestellt werden – unabhängig davon, ob gesetzlich vorgeschrieben oder unternehmenswirtschaftlich zwingend erforderlich – verhalten sich beinahe deckungsgleich. IT-Sicherheit wie Datenschutz erfüllen die Anforderungen im Unternehmen, die im Hintergrund für das operative Geschäft entscheidend sein können:

- **Vertraulichkeit** personenbezogener und aller Unternehmensdaten
- **Integrität** der verarbeiteten und übermittelten Daten und Informationen
- **Verfügbarkeit** erforderlicher Daten und Informationen im Geschäftsprozess
- **Authentizität** von Absender und Adressat beim Informationsaustausch
- **Beweiskraft** in Form – bei Bedarf juristisch -beweisfähigen Workflows

3.2 Synergie Ingenieur - Consultant

Der kritische Punkt dabei ist die Tatsache, dass von einem hochqualifizierten Administrator eine enge Spezialisierung auf sein überwiegend technisches Fachgebiet verlangt wird. Dem entsprechend verhält es sich mit seiner Qualifikation, so dass naturgemäß weder Ressourcen noch fundierte Zusatzkenntnisse in ausreichendem Maß vorhanden sein können, um den zu erwarteten neuen Erwartungen künftig gerecht werden zu können. Ein weiteres Hemmnis kann die Tatsache werden, dass IT und Management in vielerlei Hinsicht eine andere Zielsetzung verfolgen. Zum Beispiel muss der Administrator seine Ressourcen in Richtung Performance und Hochverfügbarkeit pflegen, während der Bereichsleiter ehr zum blinden Datensammeln und unspezifizierten Ablegen unverhältnismäßiger vieler Informationen neigt, die in der Praxis erfahrungsgemäß nur zu einem geringen Bruchteil genutzt werden und so unnötig die Rechner, Leitungen und die Aufmerksam des Benutzers binden, der sich durch Unmengen an Daten wühlen muss - im schlechtesten Fall sogar, ohne etwas Brauchbares zu finden.

3.3 Synergie der technisch - organisatorischen Sicherheit

An IT-Systeme werden Anforderungen gestellt, die auch der Datenschutz zum Ziel hat. Bruce Schneier, der bekannte Krypto- und IT-Sicherheits-Experte beschreibt in seinem Vorwort zu „Secrets & Lies“ (14) einen Entwicklungsprozess, den im Grunde wir alle in unseren Wirkungskreisen durchleben: „Mathematik ist perfekt; Realität ist subjektiv. Mathematik ist definiert; Computer sind störrisch. Mathematik ist logisch; Menschen sind unberechenbar, launenhaft und schwer zu durchschauen. Der Fehler in *Applied Cryptography* bestand darin, überhaupt nicht über den Zusammenhang zu sprechen. Kryptographie war für mich die Antwort auf alle Fragen. Ich war ganz schön naiv“. Schneier fordert damit gerade die Sicherheits- und Datenschutzprofis heraus, über den gewohnten Tellerrand zu Blicken, um den sich ständig erweiternden Horizont erreichen zu können, den es bedarf, um längerfristig wirksame Sicherheit der IT-Systeme und der personenbezogenen wie unternehmenssensiblen Daten gewährleisten zu können.

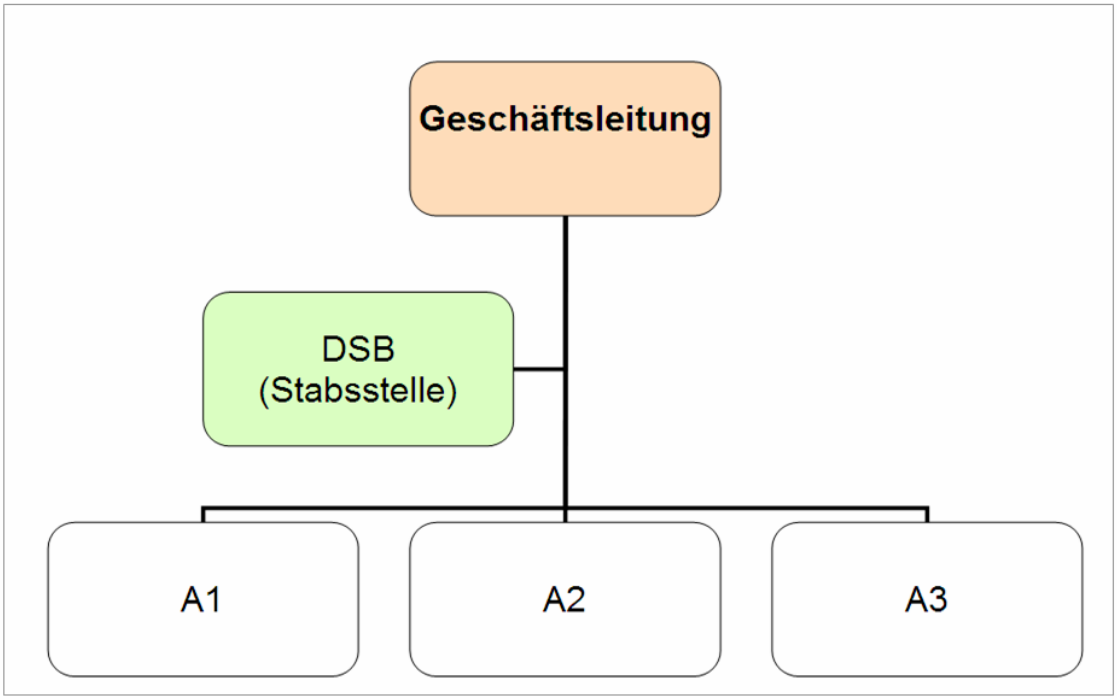

Abbildung 5: Stellung des Datenschutzbeauftragten im Unternehmen

Genau an diesem Punkt liegt für Administratoren wie ihre CIOs zugleich die größte Haftungsgefahr, da sie im Ernstfall in der Beweispflicht sind, alles getan zu haben, um ihrer Sorgfaltspflicht zu genügen. Doch wie will man in einer Disziplin, die eine solch immense Vielfalt in sich birgt, jemals beweisen, dass man genug getan bzw. etwas Falsches, das man zuvor anders eingeschätzt hat, nicht getan hat? Hier kann die Bestellung eines externen betrieblichen Datenschutzbeauftragten einen neuen frischen Blickwinkel in die Praxis einbringen, während er selbst im Gegenzug von den fundierten Erfahrungen der IT profitiert.

In vielen Fällen werden IT-Administratoren und CIOs darüber hinaus vom Unternehmen hinsichtlich ihrer Funktion und Aufgaben beschränkt, weil betriebliche Interessen temporär höher eingeschätzt werden als das Risiko, dadurch Informationen oder die Daten verarbeitenden System in ihrer Sicherheit zu gefährden. Hier kann der Datenschutzbeauftragte durch seine gesetzlich vorgeschriebene Verankerung als Stabsstelle einen kurzen Draht zum obersten Management pflegen und zugleich der IT an einigen Stellen den Rücken freihalten, wo vielen Administratoren erfahrungsgemäß zunächst die Hände von oben gebunden werden.

Der Datenschutzbeauftragte wie die IT-Kollegen profitieren gemeinsam von der Verschwiegenheitspflicht des Datenschutzbeauftragten und der parallelen Offenheit des gesamten Personalstabs, der sich ihm gerne anvertraut, sofern die Kommunikation auf allen Ebenen stimmt. Der Datenschutzbeauftragte kann konkrete „best practice“-Empfehlungen zu internen Sicherheitskonzepten abgegeben und mindert das Unternehmerrisiko durch ein passgenaues Datenschutzkonzept für das einzelne Unternehmen in seiner Gesamtheit, das sowohl technische als auch organisatorische Ansätze beinhaltet.

3.4 Praktische Ansätze zur Nutzung der Synergieeffekte

Welche Punkte für die IT-Sicherheit und den Datenschutz im Unternehmen – unabhängig von dessen Größe oder Bedeutung – juristisch und wirtschaftsökonomisch relevant sind, zeigen die Beispiele unzähliger Mitbewerber, aus deren reichem Erfahrungsschatz mit Datenschutz- und Datensicherheits-Vorfällen wir alle nahezu kostenlos schöpfen können. Öffentlichkeitswirksame Auszeichnungen wie der Big Brother Award (2), der sich zunehmender Beliebtheit in Deutschland, Österreich, Schweiz, den USA und in vielen weiteren Nationen erfreut, ist eine der Informationsquellen, an denen wir uns für die Praxis orientieren können. Die dort beschriebenen Fälle dokumentieren hervorragend, was passiert, wenn die Realität die datenschutzgesetzesresistente Geschäftsleitung trifft.

Gerade in Zeiten, wo Wirtschaftsspionage zum neuen Kavaliersdelikt zu werden scheint (8), begreifen Unternehmensverantwortliche auf allen Ebenen, welche wertvollen Betriebsgüter Daten und Informationen sein können. Entsprechend präventive Abwehrmaßnahmen sollten unverzüglich Einzug gerade in kleineren und mittelständischen Unternehmen halten, da sie durch ein weniger strenges Sicherheitskonzept schnelleren Erfolg beim Ausspähen versprechen.

4 Fazit

Professioneller Datenschutz im Unternehmen ist kein kunstvolles Konstrukt überflüssiger Prozessgarnierungen oder gar die unternehmerische „Spaßbremse“. Im Gegenteil: Wenn IT-Leiter und betrieblicher Datenschutzbeauftragter kooperativ Hand in Hand arbeiten, gut kommunizieren und komplementär wirken können, hat das klare Vorteile:

- Die wirtschaftliche Abhängigkeit des CIO und seiner IT relativiert sich im Bezug auf sicherheitsrelevante Verantwortungsbereiche, in denen der DSB durch seine Stabsfunktion ungehindert Schützenhilfe leisten kann und damit nachhaltig bewirkt, dass der verantwortungsbewusste CIO ungehindert ganze Arbeit im Sinn des Unternehmens leisten kann.
- Ein externer DSB kann CIO und IT genau an den Punkten sinn- und wirkungsvoll ergänzen, wo die aus oft langjähriger Betriebszugehörigkeit entstehende Betriebsblindheit den Blick auf potentielle Risiken trüben kann.
- Der DSB als praxisorientierter Berater wirkt sowohl betriebswirtschaftlich, sozialökonomisch, organisatorisch als auch technisch. Die IT-Sicherheit profitiert hier von den Erfahrungen anderer Aufgabenbereiche, dem fundierten interdisziplinären Gesamtüberblick des Datenschutzes in Details und dem methodischen Vorgehen des DSB.
- Potentielle Sicherheitslücken, gerade in der Nutzung automatisierter und rechnergestützter Anwendungen, die intern aus gruppendynamischen Prozessen heraus nie gegenständlich werden würden, kann der DSB auf Grund seiner intensiv-analytischen Arbeit verbunden mit der Schweigepflicht auf der Sachebene kommunizieren. Er kann damit Gelegenheit schaffen, solchen Risikoquellen wirksam zu begegnen.

Datenschutz und IT-Sicherheit profitieren gegenseitig von unzähligen Synergieeffekten, die sie in Form direkter und indirekter Vorteile an das Unternehmen weitergeben können. Der fachgerechte und rechtskonforme Umgang mit personenbezogenen und unternehmenssensiblen Daten und Informationen werden sowohl nach informationstechnischen als auch datenschutzrechtlichen Aspekten kategorisiert, Verfahrensweisen werden entwickelt und festgeschrieben, die nachhaltige Wirksamkeit entsprechender Sicherheitsmaßnahmen innerhalb der computergestützten und automatisierten Systeme sowie ihrer Anwender in Form des Personals unterliegt einer ständigen Kontrolle durch beide Instanzen und erfüllt somit zugleich das oft sinnvolle Vier-Augen-Prinzip, wenn Mitarbeiter oder andere Personen betroffen sind.

Der Betrieb profitiert zusätzlich von Transparenz und Effizienz in den Geschäftsprozessen, einem vertrauenswürdigen Image nach innen und außen, einer steigenden Sensibilität des Personalstabs für den Wert immaterieller Unternehmensgüter (Informationen und Daten), und letztlich von gesteigerter Kundenzufriedenheit. Vor allem aber schützen diese Synergien vor wirtschafsökonomischen wie juristischen Konsequenzen, die früher oder später aus der Vernachlässigung eines dieser Bereiche entstehen werden und immensen Schaden anrichten können, wenn die verantwortliche Geschäftsleitung dem nicht rechtzeitig entgegenwirkt.

Quellennachweis

(1) ASK IT-Secure GmbH: Abbildung Risikofaktoren; 07.03.2007; *http://www.serverschutzraum.de/index.php?id=69;*

(2) BigBrotherAwards: *https://www.bigbrotherawards.de;*

(3) Capgemini: Studie IT-Trends 2007 – IT ermöglicht neue Freiheitsgrade; Mai 2005; *http://www.ch.capgemini.com/m/ch/tl/IT-Trends_2005.pdf;*

(4) Capgemini: Studie IT-Trends 2005 – Paradigmenwechsel in Sicht; 09.03.2007; *http://www.ch.capgemini.com/m/ch/tl/IT-Trends_2005.pdf*

(5) Deloitte: Technology Predictions – TMT Trends 2007; 09.03.2007; *http://www.deloitte.com/dtt/cda/doc/content/dtt_%20TechPredictions011107%281%29.pdf;*

(6) Der Tagesspiegel online: Undichte Stelle gefunden - Lufthansa kündigt Mitarbeiterin wegen Bonusmeilenaffäre; 18.08.2002; *http://www.tagesspiegel.de/politik/archiv/18.08.2002/171596.asp*

(7) Europäische Gemeinschaft: 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; *http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=31995L0046&model=guichett*

(8) Financial Times Deutschland: China verschärft Wirtschaftsspionage; 08.02.2007; *http://ftd.de/unternehmen/industrie/159669.html*

(9) Gola/Schomerus: BDSG - Bundesdatenschutzgesetz Kommentar, Verlag C.H. Beck, München 2005; (und die aktualisierte Fassung von August 2006);

(10) Heilbronner Stimme: Vertrauliche Daten achtlos entsorgt; 04.08.2006; *http://www.stimme.de/nachrichten/kraichgau/art1943,839348.html?fCMS=ad4db535406bf190bbb4a93aec34448c;*

(11) Heise online: Versicherungsgruppe HUK-Coburg legte Kundendaten offen ins Netz [Update]; 06.11.2002; *http://www.heise.de/newsticker/meldung/32120;*

(12) Heise online: Vodafone Griechenland soll 76 Millionen Euro Strafe zahlen; 15.12.2006; *http://www.heise.de/newsticker/meldung/82633;*

(13) Mitnick, Kevin: Die Kunst der Täuschung – Risikofaktor Mensch, mitp-Verlag, Bonn 2003;

(14) Schneier, Bruce: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt; dpunkt.verlag GmbH, Heidelberg 2004;

(15) Spiegel Online GmbH: Polizeidaten bei ebay - Geheimes Schnäppchen; 02.04.2005; *http://www.spiegel.de/netzwelt/web/0,1518,349435,00.html;*