Ausgabe 04.13

amendos Newsletter

Liebe Leserinnen und Leser,

Cloud-Dienste sind aus der heutigen IT-Welt nicht mehr wegzudenken und werden immer häufiger in Anspruch genommen. Infolge des NSA-Skandals haben jedoch die großen US-amerikanischen Cloud-Anbieter mit starken Umsatzeinbußen zu kämpfen. In unserem ersten Artikel beleuchten wir deshalb die aktuelle und zukünftige Entwicklung des Cloud-Marktes und betrachten etwaige daraus resultierende Auswirkungen auf das Safe-Harbor Abkommen.

Corporate Governance und IT-Compliance haben sich zu zentralen Themen im Bereich der Unternehmensführung entwickelt. Doch was verbirgt sich eigentlich hinter diesen Begriffen und in welchem Zusammenhang stehen sie zueinander? In unserem zweiten Beitrag gehen wir dieser Frage anhand eines Beispiels nach.

Wir wünschen Ihnen viel Spaß beim Lesen, frohe Festtage und einen guten Rutsch ins neue Jahr!

Jörg Bujotzek
Geschäftsführer
amendos gmbh

amendos gmbh
Grüner Deich 15, 20097 Hamburg
www.amendos.de
Tel. +49 (0) 40 / 248 276 00

Cloud-Dienste in Zeiten des NSA-Skandals

Die zweite Hälfte des Jahres 2013 wird als wegweisend für die zukünftige Entwicklung des Cloud-Computing Marktes in Erinnerung bleiben. Durch die immer neuen Enthüllungen des Whistleblowers Edward Snowden hat das Vertrauen in die Cloud-Anbieter, insbesondere natürlich in die amerikanischen Größen wie Google, Amazon oder Microsoft, erheblichen Schaden genommen. Doch wie sieht die Zukunft aus? Der vorliegende Artikel beschreibt, welche Folgen der NSA-Skandal für Anbieter und Nutzer von Cloud-Diensten hat, wie die Entwicklung des zukünftigen Cloud-Marktes aussehen kann sowie die Auswirkungen der Spähaffäre auf das Safe-Harbor Datenschutzabkommen.

Laut der Information Technology & Innovation Foundation (ITIF), einem der bedeutendsten Technologie-Thinktanks, könnten die Enthüllungen der NSA-Ausspähungen die amerikanischen Cloud-Dienstleister in den kommenden zwei bis drei Jahren bis zu 35 Milliarden Dollar an Umsatzeinbußen kosten. Ein Fünftel der Marktanteile im Ausland sind bedroht. Das Marktforschungsunternehmen Forrester Research beziffert den möglichen Schaden gar auf 180 Milliarden Dollar. Einer Umfrage unter den Mitgliedern der Cloud Security Alliance zufolge, hätten 10 Prozent der ausländischen Kunden bereits bestehende Cloud-Projekte abgebrochen, 56 Prozent bezeichneten es wegen der NSA-Enthüllungen als unwahrscheinlich, in Zukunft auf US-Anbieter zurückzugreifen.

"Worst-Case" Verlust-Szenario (in Mrd. US Dollar)			
	2014	2015	2016
Globaler Cloud-Markt	$148.9	$160.0	$207.0
US-Cloud-Markt	$72.9	$75.2	$93.2
Nicht-US-Cloud-Markt	$75.9	$84.8	$113.9
Anteil von US-Cloud-Anbietern am nicht-US-Markt (vor PRISM)	85%	80%	75%
Anteil von US-Cloud-Anbietern am nicht-US-Markt (nach PRISM)	80%	70%	55%
Umsatz von US-Cloud-Anbietern am nicht-US-Markt (vor PRISM)	$64.5	$67.8	$85.4
Umsatz von US-Cloud-Anbietern am nicht-US-Markt (nach PRISM)	$60.7	$59.4	$62.6
Jährlicher Verlust	$3.8	$8.5	$22.8
Gesamtverlust über 3 Jahre	$35		

Abbildung 1: Erwartete Verluste der US-Cloud-Anbieter gemäß ITIF (Zahlen von Gartner Inc.)

Auswahlkriterien für einen Cloud-Anbieter waren bisher überwiegend der Bedienkomfort und natürlich der Preis. In Zukunft jedoch wird es bei der Auswahl auch darum gehen, wie gut die Verschlüsselung ist und wo sich die Rechenzentren befinden. Für Google z. B. ist die Verschlüsselung allerdings ein Problem. Googles Geschäftsmodell basiert auf der Durchsuchbarkeit und Analyse von Daten. Verschlüsselte Daten jedoch lassen sich weder durchsuchen noch analysieren.

Bei deutschen Cloud-Anbietern hingegen herrscht Hochstimmung. Das Hamburger Unternehmen Cloudsafe registrierte einen Zuwachs von 25%. Insbesondere die Nachfrage aus den USA legte stark zu, gerade weil das Hosting in Deutschland stattfindet. Umgekehrt scheuen viele deutsche Unternehmen nun das Risiko, einen ausländischen Dienstleister einzusetzen.

Auch Anbieter die Open-Source-Programme für ihre Clouds verwenden, wie zum Beispiel Metaways, spüren einen Nachfrageanstieg, weil es bei Open Source Programmen keine versteckten Hintertüren geben kann, da der Programmcode einsehbar ist. Allerdings haben Open-Source-Programme immer den Nachteil der mangelnden Kompatibilität mit etablierten, weltweit eingesetzten Standards, wie z. B. den Produkten von Adobe oder Office von Microsoft.

Doch was wurde seitens der NSA überhaupt ausspioniert? Laut Dokumenten von Edward Snowden bestand beispielsweise der Angriff auf Google darin, den Datentransfer zwischen den Google-Rechenzentren, welcher zwar in einem eigenen Netzwerk, aber leider unverschlüsselt abgewickelt wurde, auszuspähen. Weiterhin wurde öffentlich, dass die großen US IT-Firmen gerichtlich gezwungen wurden, die NSA mit Informationen zu versorgen.

Wie gehen diese Schwergewichte unter den Cloud-Anbietern nun mit dem Vertrauensverlust um? Bei nahezu allen Unternehmen wurde der IT-Etat, vor allem mit Blick auf die Datensicherheit, stark aufgestockt. Google kündigte an, den Datentransfer zwischen den Rechenzentren zu verschlüsseln, Yahoo kündigte das gleiche Vorgehen für seinen E-Mail Dienst an. Microsoft und Google haben bereits im Juni 2013 Klage gegen die US-Regierung hinsichtlich mehr Informationstransparenz eingereicht. Der Redmonder Softwarekonzern ist eines der am stärksten von dem NSA-Skandal betroffenen Unternehmen, da das Ausspähprogramm sowohl eines der wichtigsten Produkte als auch die zentrale Strategie für die Zukunft betraf: Office365. Die weltweit am meisten verbreitete Office Software soll in die Cloud wandern, sowohl Standard Programme an sich (Word, Excel, PowerPoint) als auch die Dienste wie Exchange, Lync oder SharePoint. Kunden sollen nicht nur via Cloud auf die Programme zugreifen, sondern auch die unternehmenseigenen Dokumente bei Microsoft ablegen, dies selbstverständlich ebenfalls in der Cloud. Microsoft versucht dem entstandenen Vertrauensverlust entgegenzuwirken, indem darauf hingewiesen wird, dass die Server in der EU – in Irland – stehen und somit also vor dem Zugriff von US-Geheimdiensten geschützt sind. Auch wird gern mit der vorhandenen Safe-Harbor Zertifizierung geworben. Doch was ist Safe-Harbor überhaupt?

Bei Safe-Harbor handelt es sich um eine Vereinbarung, welche im Jahr 2000 zwischen der Europäischen Union und den USA getroffen wurde. Das Abkommen erlaubt und regelt unter bestimmten Umständen die Weitergabe personenbezogener Informationen aus EU-Mitgliedsstaaten an Unternehmen in den USA. Die Übereinkunft erlaubt Firmen einen Datentransfer über den Atlantik, wenn sie dort ein angemessenes Schutzniveau bereithalten. Das Abkommen war nötig geworden, da zur Jahrtausendwende die EU-Datenschutzrichtlinien reformiert wurden. Diese Reform zog das Verbot nach sich, personenbezogene Daten in Staaten zu transferieren, welche kein dem EU-Recht vergleichbares Datenschutzniveau haben. Einer der von diesem Verbot betroffenen Staaten sind die USA. Um den Datenverkehr zwischen den USA, der EU und später auch der Schweiz nicht zum Erliegen zu bringen, wurde auf Grundlage der sogenannten „Safe-Harbor Principles“ ein Verfahren entwickelt, welches den Datenverkehr rechtlich wieder ermöglicht.

Zu den anzuwendenden Grundsätzen gehören etwa der der Transparenz, der Zweckmäßigkeit der Informationsverarbeitung, der Datensicherheit sowie der Korrigierbarkeit der erfassten Informationen. Dem Safe-Harbor Abkommen beitreten können Unternehmen, die sich auf einer entsprechenden Liste des US-Handelsministeriums eintragen lassen. Zu den Teilnehmern gehören Konzerne wie Amazon, Facebook, Google, Hewlett-Packard, IBM oder Microsoft. Eingetragene Firmen können dann mit einem entsprechenden Logo werben. Es handelt sich bei Safe-Harbor allerdings nicht um einen völkerrechtlichen Vertrag, sondern lediglich um eine Vereinbarung. Ein weiteres Problem

dieses Abkommens ist, dass es seit 2001 vom sogenannten „Patriot Act“ gleichsam überstimmt wird. Dieses Gesetz, verabschiedet nach den Terroranschlägen vom 11. September 2001, sieht vor, dass US-Unternehmen verpflichtet sind, im Anforderungsfall Daten auch von Cloud-Servern, selbst von solchen die in der EU stehen, an die amerikanischen Behörden weiterzugeben. Rein europäische Cloud-Anbieter, die nicht an den Patriot-Act gebunden sind, haben aufgrund dieses Umstandes einen großen Vertrauensvorteil gegenüber der US-Konkurrenz.

Lesen Sie hierzu auch:

Newsletter Ausgabe 02/2013

- Die Cloudlösung Office 365 im Unternehmenseinsatz – ein Überblick

Auch wenn es gegenüber Safe-Habor viele Einwände gibt, halten Datenschützer dieses Abkommen dennoch weiterhin für berechtigt. Selbst wenn demnächst die geplante EU-Datenschutzreform verabschiedet würde und diese einen Transfer personenbezogener Informationen in Drittstaaten im Wirtschaftsbereich transparenter mache oder einschränke, könne ein solcher Datenaustausch in der global vernetzten Wirtschaft doch nicht ganz untersagt werden ohne mit erheblichen Konsequenzen für diese zu rechnen. Ein Großteil der Informationen werde folglich weiter in die USA, in die dort betriebenen Clouds, gehen, aber auch nach China oder Indien, die ebenfalls auf den Cloud-Markt drängen. Außerdem erscheint es fragwürdig, ob ein Aussetzen oder Aufkündigen des Abkommens Spionage unterbinden würde, schließlich sind Überwachungsprogramme wie „PRISM“ oder „XKeyScore“ nicht auf irgendwelche Vereinbarungen angewiesen.

Fazit:

Es wird einige Zeit dauern, bis das zerstörte Vertrauen in die Cloud halbwegs wieder hergestellt ist. Aufzuhalten ist der Trend zur Datenwolke jedoch nicht. Ausschlaggebend für diese Entwicklung sind Faktoren wie Kosteneinsparungen und Vereinfachung der Wartung. Allerdings werden sich künftige Auslagerungsprojekte viel stärker mit Punkten wie Datensicherheit und Verschlüsselung auseinandersetzen müssen als bisher. Auch der Standort der Server wird noch stärker in den Fokus rücken. Amerikanische Anbieter sind hier, trotz Safe-Harbor Vereinbarung, klar benachteiligt. Selbst wenn zum Beispiel Microsoft betont, dass die Office365 Server in Irland und somit nicht im direkten Zugriffsbereich von US-Geheimdiensten stehen, wird der NSA-Skandal den US-amerikanischen Cloud-Anbietern noch lange anhaften.

Michael Pfitzmann

Von der Corporate Governance zur IT-Compliance

Corporate Governance und IT-Compliance sind unscheinbare Begriffe aus dem Business Umfeld, mit deren Definitionen und Interpretationen sich dennoch unzählige Diskussionsseiten im Internet befassen. Es wird gewissermaßen mehr Energie darauf verwendet, die Definition zu perfektionieren als deren inhaltlichen Belangen konsequent nachzugehen. Dieser Artikel soll anhand eines Beispiels die Bedeutung und den Zusammenhang einfach veranschaulichen.

Der Begriff Compliance ist laut Duden mit vier verschiedenen Bedeutungen belegt. Die wohl zutreffendste im IT-Zusammenhang ist „(Wirtschaftsjargon) regelgerechtes, vorschriftsgemäßes, ethisch korrektes Verhalten“. Der Begriff Corporate Governance hingegen taucht gar nicht erst im offiziellen deutschen Sprachschatz auf. Wörtlich übersetzt würde er Unternehmensregierung bedeuten. Man kann ihn aber eher mit Regeln der „guten“ Unternehmensführung gleichsetzen.

Was verbirgt sich hinter diesen Regeln und was ist das eigentliche Ziel, welches damit verfolgt wird? Im Kern geht es zunächst um „gesunden Menschenverstand“ in der Unternehmensführung und ein ausgewogenes Maß in der Adressierung betriebswirtschaftlicher und gesellschaftlicher Anforderungen.

Braucht es nun aber eine Regierung oder Behörde um dieses Maß zu finden? Betrachtet man z.B. den Hintergrund des in Europa eingeführten und den nationalen Gegebenheiten angepassten Deutschen Corporate Governance Kodex, so wird schnell deutlich, dass hiermit auch andere Ziele anvisiert werden. Investoren soll vermittelt werden, dass hier ansässige Aktiengesellschaften eine Unternehmensführung besitzen, die für eine angemessene Transparenz und Investitionssicherheit Sorge trägt. Dieses Beispiel zeigt, dass es durchaus unterschiedliche Auslegungen des Kozeptes „Corporate Govenance“ gibt: Während einige Unternehmen darin eher ein Marketinginstrument sehen, verstehen es andere als Regelwerk zur Verbesserung des gesellschaftlichen und nachhaltigen Miteinanders. Es existiert sogar eigens eine Regierungskommission um diesen Kodex zu überwachen.

amendos Spezial Outsourcing – Teil1

Outsourcing von Teilen der eigenen IT-Leistungen ist in Unternehmen und öffentlichen Einrichtungen keine Seltenheit mehr. Deshalb ist es umso erstaunlicher, dass viele Outsourcing-Vorhaben nicht den geplanten wirtschaftlichen Erfolg erzielen. Die Gründe hierfür sind vielfältig.

In dieser Ausgabe von **amendos Spezial** dreht sich daher alles um

„Outsourcing“:

- Risikoanalyse für IT-Outsourcing-Projekte
- Einholung von Angeboten
- Mindestanforderungen bei der Erstellung von Lastenheften
- Vermeidung von Fallstricken in der Transition

amendos Spezial PM – Methoden

Fundament für ein professionelles Projektmanagement in Unternehmen ist die Etablierung einheitlicher PM -Methoden und -Tools sowie deren kontinuierliche Weiterentwicklung.

In dieser Ausgabe von **amendos Spezial** dreht sich daher alles um

„Projektmanagement – Methoden“:

- Rolle von PM-Methoden
- PM-Erfolgsfaktoren
- Projektcontrolling
- „klassisch vs. agil“?

Ist so viel Aufwand wirklich nötig um etwas zu regulieren, was es schon immer gab? Offensichtlich – ja. Die Globalisierung sowie die extrem schnelllebigen Märkte zwingen Unternehmen, dieses Thema strukturierter und vielleicht auch regulierter als noch vor 50 Jahren anzugehen. Ein Unternehmen steht heutzutage mehr denn je im Fokus der Öffentlichkeit. Nachrichten über ethisch fragwürdige oder nachlässige Geschäftspraktiken wie z.B. die Bezahlung von Niedriglöhnen oder Datenpannen verbreiten sich binnen Minuten im Internet und können ein Unternehmen massiv in Bedrängnis bringen. Eine Corporate Governance soll solche und weitere Risiken minimieren, indem zuerst das Umfeld analysiert und auf Basis der Ergebnisse Regelungen definiert werden, um in diesem zu bestehen.

Eine Corporate Governance wird maßgeblich geprägt durch drei Themenfelder: die rechtlichen nationalen und internationalen Regelungen, die betriebswirtschaftlichen und strategischen Ziele sowie gesellschaftliche Rahmenparameter. Erst nachdem dieses komplexe Umfeld erfasst, analysiert und eine Corporate Governance aufgestellt wurde, kann daraus auch eine ganzheitliche IT-Governance abgeleitet werden. In dieser ist beschrieben wie die IT die Unternehmensstrategie unterstützen und Unternehmenswerte schützen soll. Die IT-Compliance ist ein wesentlicher Bestandteil der IT-Governance. Sie stellt sicher, dass die IT „compliant“ gegenüber den in der Corporate Governance identifizierten Regeln agiert und implementiert angemessene Maßnahmen, um die Unternehmenswerte zu schützen. Um den Schutzbedarf zu quantifizieren, bedarf es eines soliden Risikomanagements, das die Gefahren, denen die Werte unterliegen, analysiert und entsprechende Maßnahmen ableitet. Danach existiert eine Basis um IT-Compliance auch bewertbar zu machen. Ohne diese Voraussetzung ist es nicht möglich einzuschätzen, ob Aufwendungen, z.B. zur Einhaltung von gesetzlichen Vorgaben, verhältnismäßig und ausreichend sind.

Die IT-Compliance hat als Antriebsmotor die Ergebnisse der Risikoanalyse und befasst sich damit, angemessene und adäquate Mechanismen zu implementieren, um die geplanten Maßnahmen umzusetzen. Folgendes sehr vereinfachtes Beispiel soll diesen Entstehungsprozess für eine einzelne Maßnahme veranschaulichen.

Ein internationaler IT-Konzern, der u.a. auch Cloud-Dienste anbietet, überarbeitet seine Corporate Governance und überprüft, ob sie noch der heutigen Marksituation gerecht wird. Dabei wird festgestellt, dass durch die andauernde öffentliche Diskussion über Spionagefälle das Misstrauen der deutschen Kunden gegenüber der Informationstechnologie extrem gestiegen ist. Insbesondere die Speicherung sensibler personenbezogener Daten im amerikanischen Raum wird von vielen deutschen Kunden als nicht mehr tragbares Risiko gesehen. Auch die gültigen Abkommen wie Safe-Harbor, die sicherstellen sollten, dass auch in den USA für diese Daten nationale Datenschutzbestimmungen gelten, ändern daran nichts. Diese basieren auf einer freiwilligen Verpflichtung der dortigen Anbieter und können durch amerikanische Gesetze wieder ausgehebelt werden.

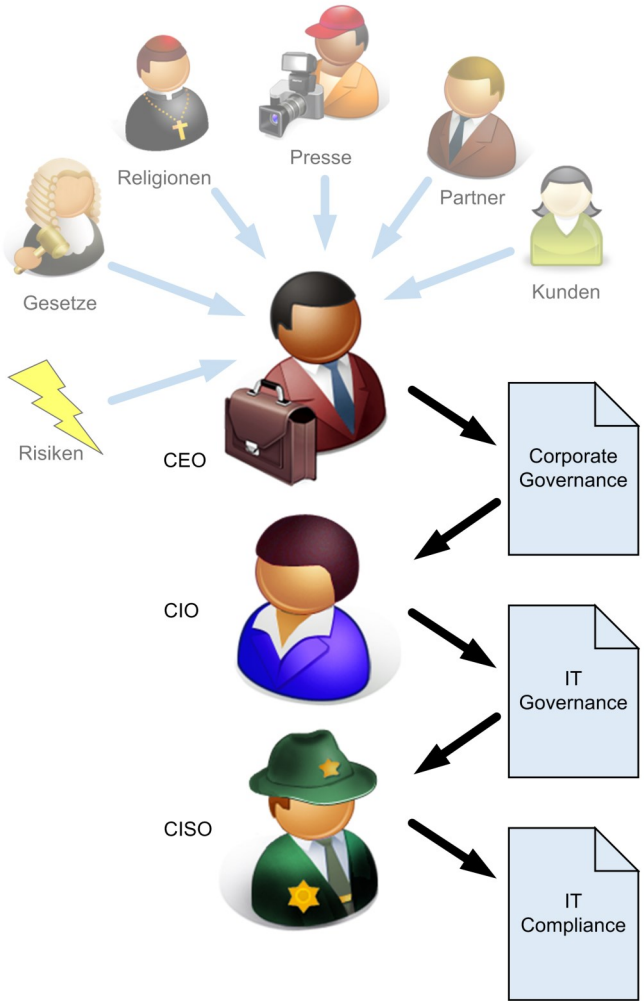
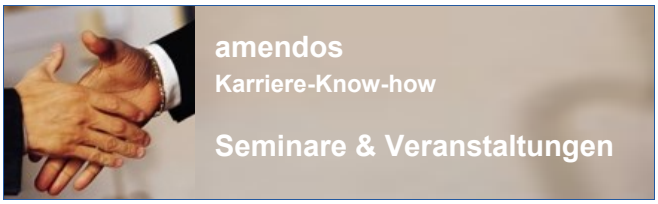


Abbildung 1: Von der Corporate Governance zur IT-Compliance

Das Unternehmen ist aus betriebswirtschaftlicher Sicht natürlich daran interessiert, sich am Markt zu behaupten. Deshalb muss auf den aktuellen gesellschaftlichen Wandel in Bezug auf die steigende Skepsis reagiert werden. Die deutsche Gesetzgebung verschärft diese Situation zusätzlich, indem z.B. die Speicherung steuerlich relevanter Daten ausschließlich im EU Wirtschaftsraum und auch nur nach vorheriger Genehmigung der



Seminare 1. Halbjahr 2014

Projektmanagement	**Intensiv Seminar Projektmanagement** Hamburg, tba **Kommunikationskompetenz in Projektkrisen** Hamburg, 22.01. – 23.01.2014 **Project Management Offices im IT-Umfeld** Hamburg, 05.03. – 07.03.2014 **Soft Skills für Projektleiter/innen** Hamburg, 25.03. – 26.03.2014 **IT-Projekte erfolgreich aus der Krise führen** Hamburg, 25.06. – 26.06.2014
IT SM	**Einführung in die Prozessoptimierung** Hamburg, 30.01. – 31.01.2014 **Prozessdokumentation gestalten** Hamburg, 06.02.2014 **Erstellung von IT-Servicekatalogen** Hamburg, 28.04.2014 **IT-Providermanagement** Hamburg, 15.05.2014
Outsourcing	**Ausschreibung von IT-Dienstleistungen** Hamburg, 20.02.2014 **IT-Ausschreibung mit Finanzierungsoptionen** Hamburg, 20.03. – 21.03.2014 **Outsourcing von Workplace Services** Hamburg, 10.04.2014
ITK	**Cloud Computing Overview** Hamburg, 05.05.2014 **VoIP Überblick und Konzepte** Düsseldorf, 10.06. – 11.06.2014

Seminare: Info & Anmeldung
www.amendos.de/seminare
Tel (040) 248 276-00, info@amendos.de

Finanzbehörden erfolgen darf. Hier zeichnet sich ein konkretes Risiko ab: die entsprechende Kundengruppe wird weniger oder gar keine der angebotenen Cloud Lösungen mehr nutzen. In die überarbeitete Corporate Governance wird nun aufgenommen, sich nationalen Anforderungen im IT-Sicherheitsumfeld intensiver zu widmen. Es sollen transparente Lösungen geschaffen werden, die das Unternehmen so am Markt etablieren, dass es sich im IT-Sicherheitsumfeld von der Konkurrenz positiv abhebt. Als Maßnahme wurde definiert, die rechtlichen und technischen Gegebenheiten des eigenen Serviceangebots daraufhin anzupassen.

Der erste Schritt ist, eine deutsche GmbH auszugründen, die damit für Kunden eindeutig sichtbar dem deutschen Recht unterliegt. Der vermeintliche sichere Anbieter würde aber schnell an Akzeptanz verlieren, wenn sich herausstellt, dass die Daten im Rechenzentrum des amerikanischen Mutterkonzerns liegen. Weshalb auch noch eine zweite, technische Maßnahme von Nöten ist: die Schaffung nationaler Rechenzentren. Nun ist es aber für dieses vergleichbar kleine Unternehmen nicht möglich, eine mit dem Mutterkonzern vergleichbare komplette Betriebsorganisation zu stellen. Die favorisierte Lösung in diesem Fall ist das Outsourcing der betreffenden Leistungen. Entscheidend ist jetzt, dass die eingekauften Dienste neben den typischen Faktoren wie Verfügbarkeit, Kosten usw. vor allem eine Anforderung erfüllen: eine nachweislich ausnahmslose Speicherung der Daten auf deutschem Bundesgebiet.

Diese kleine Nuance ist aus technischer und rechtlicher Sicht nicht zwingend erforderlich. Aber dadurch, dass diese Anforderung in der Corporate Governance begründet ist, wird sie entscheidend, um „compliant“ zu sein.

Fazit:
Im IT Jargon werden immer wieder neue Begriffe Einzug halten, (IT-) Governance und (IT-) Compliance sind aber bereits feste Bestandteile. Entscheidend für den Umgang mit den dahinterstehenden Konzepten ist jedoch nicht, die treffendste Definition der beiden Begriffe zu kennen, sondern die dahinterstehenden Werte und Ziele zu leben. Jedes etablierte Unternehmen hat eine mehr oder weniger umfangreich definierte Corporate Governance, ob sie nun auch so benannt ist oder nicht. Ein Verantwortlicher im IT Umfeld sollte daher immer im Auge behalten, ob die von ihm verantwortete IT-Compliance auch wirklich alle Anforderungen der aus der Unternehmensstrategie abgeleiteten Corporate Governance optimal und präzise unterstützt.

Henry Wudi

Impressum

amendos gmbh I Grüner Deich 15 I 20097 Hamburg
Tel (040) 248 276 00 I Fax (040) 248 276 01 I www.amendos.de I info@amendos.de I Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917

Erscheinungsweise 4 / jährlich I Bezug: kostenfrei als PDF I Copyright: amendos gmbh
Herausgeber und inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV: Dipl. Oec. Jörg Bujotzek