Cloud-Angebote und IT-Compliance

Jan Philipp Timme

Hochschule Hannover, Hannover, Deutschland,
jan-philipp.timme@stud.hs-hannover.de,
Website: http://www.hs-hannover.de

Zusammenfassung. IT-Compliance gewinnt zunehmend an Bedeutung und ist aus Unternehmen kaum noch wegzudenken. In diesem Dokument werden die Aufgaben von IT-Compliance erläutert und Anhand der ISO 27001 gezeigt, welche Vorteile IT-Compliance einem Unternehmen bringen kann. Auch die Relevanz der ISO 27001 für Cloud-Angebote wird erläutert.

Schlüsselwörter: IT-Compliance, ISO 27001, Compliance, Cloud-Angebote, Compliance Management System, Zertifizierung, Datensicherheit, Sicherheitsrisiken, Information Security Management System

1 Compliance und IT-Compliance

Bei *Compliance* handelt es sich um einen Begriff aus der betriebswirtschaftlichen Fachsprache. Das englische Wort „Compliance“ bedeutet übersetzt soviel wie Einhaltung, Befolgung, Regelkonformität. Das dazugehörige Verb „to comply“ steht für einwilligen, nachgeben, den Auflagen entsprechen.

Der Begriff Compliance bedeutet also die Einhaltung von Gesetzen und Vorschriften im Unternehmen[Wika]. Beispiele hierfür sind Gesetze wie die Abgabenordnung (AO), das Jugendarbeitsschutzgesetz (JArbSchG) oder das Bundesdatenschutzgesetz (BDSG). Neben Gesetzen müssen Unternehmen sich in der Regel noch an weitere Regeln und Richtlinien halten, wie zum Beispiel EU-Richtlinien, internationale Konventionen oder Normen.

Die Menge der zu berücksichtigenden Regeln ist von dem konkreten Unternehmen abhängig, welches Compliance erreichen möchte. Ab einem gewissen Umfang ist hierfür juristische Unterstützung (beispielsweise durch Beratung) notwendig. Je nach Größe des Unternehmens reichen mögliche Optionen hierfür von dem Einkauf juristischer Beratung über das Einstellen eines Mitarbeites für juristische Fragen bis zum Aufbau einer eigenen Rechtsabteilung. Hierbei ist direkt ersichtlich, dass in jedem Fall erste Kosten entstehen, die direkt mit durch das Anstreben von Compliance verursacht werden.

Nachdem ein erster Einstieg in die Welt der Compliance erfolgt ist, kommt nun schnell die Frage auf, wie man durchgehend sicherstellen kann, dass man Regelkonform mit dem Unternehmen unterwegs ist. Hier stellt das *Compliance Management System* (CMS) ein betriebswirtschaftliches Werkzeug dar, welches genau diesen Zweck verfolgt[Wikb]. Es beinhaltet Maßnahmen und Prozesse zur

Sicherstellung von Regelkonformität im Unternehmen und integriert sich hierfür unter anderem in Unternehmensprozessen.

Ziel des CMS ist es, Risiken für Regelverstöße rechtzeitig zu erkennen, diese zu analysieren und Maßnahmen zu ergreifen, um die Risiken zu vermeiden. Sollte es nicht möglich sein, einen Regelverstoß zu vermeiden, so bietet das CMS an dieser Stelle die Möglichkeit, angemessen auf den Umstand zu reagieren und somit angebracht Schadensbegrenzung zu betreiben. Durch die Integration eines CMS im Unternehmen entsteht natürlich ein erhöhter Aufwand für alle Mitarbeiter, welches wiederrum zu erhöhten Kosten führt. Allerdings ist an dieser Stelle nicht zu vernachlässigen, dass durch die Risikoanalyse und aktive Minimierung von Risiken langfristig Kosten — ähnlich wie bei einer Versicherung — vermieden werden.

Begriff: IT-Compliance Nachdem nun der Grundbegriff der Compliance aus dem Kontext der BWL eingeführt wurde, soll nun auf *IT-Compliance* eingegangen werden. IT-Compliance ist Compliance konkret für den IT-Bereich und betrifft die Prozesse und Systeme der IT des Unternehmens. Dabei sollen die folgenden Kern-Anforderungen durch IT-Compliance umgesetzt werden[Wikd]:

- Informationssicherheit
- Verfügbarkeit
- Datenaufbewahrung
- Datenschutz

IT-Compliance minimiert Risiken im IT-Betrieb im Unternehmen, bringt allerdings ebenso wie Compliance zusätzliche Kosten mit sich. Laut einer Studie von CSC[Cor] fließen ca. 2/3 des IT-Budgets einer Bank in IT-Compliance und Instandhaltung von Systemen; je nach Unternehmen kann IT-Compliance also zu einer größeren Belastung führen.

Die Einhaltung von Gesetzen oder Vorschriften wird nicht belohnt, allerdings führen Verstöße gegen Gesetze oder Vorschriften häufig zu Strafen. Diese können wirtschaftliche Folgen für das Unternehmen in Form von Bußgeldern, Gewinnabschöpfungen oder Gewinnverfall haben, oder sogar zu Haftstrafen führen. (Beispielsweise für den Vorstand einer AG oder den Geschäftsführer einer GmbH) Neben den direkten Kosten der Strafe wird das Unternehmen allerdings auch von Kosten durch Folgeschäden belastet. Diese Folgeschäden beinhalten unter anderem Verfahrenskosten, Schadenersatzansprüche, Rückabwicklungen, Imageverluste und Vertrauensverluste. Je nach Schwere der Folgeschäden kann dies für ein Unternehmen eine Existenzbedrohung darstellen, somit ist IT-Compliance (und Compliance) ein grundlegendes Unternehmensziel.

Vorteile von IT-Compliance Das Einführen von IT-Compliance bringt Vorteile mit sich, die sich hauptsächlich mit Risikominimierung durch vorausschauendes Handeln befassen. So wird innerhalb des Unternehmens durch frühzeitige Betrachtung von relevanten Gesetzen und Risiken ein Risikobewusstsein geschaffen. Durch strukturiertes Vorgehen wird auch Datensicherheit geschaffen.

Nach außen hin schafft IT-Compliance Vertrauen bei Vertragspartnern und Kunden und demonstriert Stabilität und Robustheit des Unternehmens. Weiterhin ist es dem Unternehmen möglich, Garantien bezüglich der Datensicherheit auszusprechen, sowie Anforderungen von Kunden oder Vertragspartnern diesbezüglich zu erfüllen. Es bleibt einzig und allein das Problem, wie die IT-Compliance einem Kunden oder Vertragspartner gegenüber nachgewiesen werden kann. Hierrauf wird in Kapitel 3 näher eingegangen.

2 Cloud-Angebote

Der Begriff *Cloud-Angebote* ist ein von Kontext und Betrachtung abhängiger Begriff. Im Kontext dieses Dokuments beschreibt er Dienstleistungen eines Anbieters, welcher virtuelle Maschinen, Speicher, Anwendungen und Plattformen einem Kunden „on demand“ zur Verfügung stellt. Charakteristisch für diese Art von Dienstleistung ist die dynamische Anpassbarkeit des Leistungsumfangs, sowie die dynamischen Tarife, nach denen die Leistung dem Kunden berechnet wird.

Bietet ein Anbieter Cloud-Angebote an, so verfügt er über eine technische Infrastruktur, die auf Rechenzentren in mehreren verschiedenen Ländern weltweit verteil ist, welche global vernetzt sind. Somit werden Daten, welche im Rahmen einer solchen Dienstleistung vom Kunden abgelegt werden weltweit verteilt gespeichert. Da je nach Standort der einzelnen Rechenzentren unterschiedliche Gesetze und Vorschriften gelten, ergeben sich hierfür gleich mehrere Problemstellen.

Aus Perspektive eines Kunden von Cloud-Angeboten ergibt sich die Nutzung dieser Angebote oft aus dem Willen, Kosten einzusparen. Kostet die eigene IT-Infrastruktur in Verbindung mit der dafür nötigen IT-Compliance zu viel, so kann es sich lohnen, die benötigten Dienste durch ein Cloud-Angebot zu ersetzen. Hierbei ist jedoch kritisch, dass die benötigten Anforderungen an die Datensicherheit eingehalten werden. Möchte beispielsweise eine deutsche Versicherung ihre Kundendaten in die Cloud verschieben, so muss weiterhin darauf geachtet werden, dass das Bundesdatenschutzgesetz eingehalten wird. Des weiteren müssen die Kundendaten vertraulich bleiben, jederzeit verfügbar sein und nicht außerhalb von Deutschland gespeichert werden. Sucht ein Kunde nun international einen Anbieter mit diesen Kriterien, so ist es notwendig, dass der Anbieter diese Anforderungen belegbar erfüllen kann.

Aus Perspektive des Anbieters ergibt sich aus der Verpflichtung, alle Gesetze und Vorschriften der verschiedenen Länderstandorte zu erfüllen, eine sehr große Herausforderung. Je mehr Standorte sich in unterschiedlichen Ländern befinden, desto mehr Gesetze finden Anwendungen und die Komplexität steigt. IT-Compliance sichert an dieser Stelle die eigene Existenz des Unternehmens des Anbieters, da mit einer solchen Menge an Gesetzen viel mehr Risiken verbunden sind, dass diese nicht eingehalten werden können.

Hinzu kommt, dass Kunden aus unterschiedlichen Ländern gegebenenfalls unterschiedliche Rechte genießen, mit denen die Angebote des Anbieters ent-

sprechend übereinstimmen müssen. Da die Kunden oft auch Anforderungen an die Datensicherheit haben, muss der Anbieter die Einhaltungen dieser belegen können. Um Kunden zu gewinnen und zu überzeugen, möchte der Anbieter dementsprechend in der Lage sein, weltweit nachweisen zu können, dass sein Unternehmen einen bestimmten Grad an Datensicherheit gewährleisten kann.

3 ISO 27001

Steckbrief: ISO 27001 Die ISO 27001 ist ein international anerkannter Standard und wurde erstmals im Jahr 2005 definiert.Später wurde sie dann im Jahr 2013 generalüberholt und seit dem nur noch leicht angepasst[ISO13]. Sie definiert Anforderungen und dazu passende Kontrollen an ein *Information Security Management System* (ISMS), welches einen Ähnlichen Ansatz wie das Compliance Management System verfolgt. Der Fokus des ISMS liegt auf Datensicherheit; genauer dem Bewahren der Vertraulichkeit, Integrität und Verfügbarkeit von Daten durch Anwendung von Risikomanagementprozessen. Je nach Struktur und Bedarf des Unternehmens sind Struktur und Aufbau des ISMS unterschiedlich. Im Vergleich zur regulären IT-Compliance bietet die ISO 27001 jedoch den Vorteil, dass man sich nach ihr zertifizieren lassen kann.

Für den Aufbau des ISMS wird ein „Top-Down"-Ansatz verfolgt, welcher sich auch im Dokument der ISO 27001 widerspiegelt. Ein Satz in diesem Dokument beginnt sehr häufig mit „Top management shall ensure that ... "[ISO13]. Ein Auszug der Anwendungsgebiete des Dokuments sieht wie folgt aus[Wikc]:

- Managen von **Sicherheitsrisiken**
- Sicherstellung der Einhaltung von Gesetzen und Vorschriften
- Definition von Managementprozessen zum Managen von Informationssicherheit
- Nutzung durch Auditoren als „Checkliste"

Neben dem Aufbau des ISMS wird auch die Erzeugung und kontinuierliche Pflege einer Datensicherheitsrichtlinie beschrieben.

Auswirkungen der ISO 27001 Baut man mit Hilfe der ISO 27001 ein ISMS im Unternehmen auf, so integriert sich dieses ähnlich wie bei IT-Compliance in das Unternehmen und nimmt so Einfluss auf den Entwurf neuer Prozesse und Informationssysteme oder Kontrollen und berücksichtigt Ziele und Risiken rund um Datensicherheit von Beginn an mit. Durch diesen Aufwand werden neben internen Kosten durch den Aufbau des ISMS und der zugehörigen Dokumentation auch weitere Kosten durch Beauftragung von Beratungsunternehmen und Audit Kosten durch Zertifizierungsunternehmen verursacht. Somit ist die volle Umsetzung der ISO 27001 im Unternehmen deutlich teurer im Vergleich zu IT-Compliance mit einem CMS.

Im Gegensatz zu „regulärer" IT-Compliance ist es mit der ISO 27001 jedoch möglich, die Konformität zu zeigen. So ist es möglich, sie selbst zu verkünden oder Kunden beziehungsweise Vertragspartner zu bitten, die Konformität zu

bestätigen. Oft wird jedoch die Verifikation der Konformität durch einen externen Auditor angestrebt. (Zertifizierung nach ISO 27001)

Nutzen der ISO 27001 Hat man die ISO 27001 in seinem Unternehmen umgesetzt, so ergibt sich eine langfristige Kostensenkung durch strukturierte Prozesse und die Risikominimierung. Diese führt zu geringeren Haftungs- und Geschäftsrisiken, geringeren Versicherungsbeiträgen und verbesserter Kreditwürdigkeit bei Banken und Investoren. Auch ergibt sich eine höhere Wettbewerbsfähigkeit und Imageverbesserung durch die belegbare Datensicherheit.

Als international anerkannter Standard kann ein Cloud-Anbieter nun weltweit seine Konformität belegen. Die Zertifizierung erhöht das Vertrauen der Kunden, außerdem kann nun belegt werden, dass die Anforderungen der Kunden erfüllt werden. Regelmäßige Audits stellen die Konformität sicher und erhöhen die Transparenz, somit können Kunden ohne Sorgen die Dienstleistungen des Anbieters nutzen.

4 Umsetzung von Compliance

Nachdem Compliance zuvor beschrieben wurde, soll nun dargestellt werden, auf welchem Weg Compliance in ein Unternehmen gelangt und welche Rolle die Mitarbeiter des Unternehmes dabei spielen. Es beginnt mit der Einführung des Compliance Management Systems durch das Mangement des Unternehmens. Die Prozesse des Unternehmens werden angepasst und es werden mehr Kontrollmechanismen eingeführt. Im Idealfall akzeptieren die Mitarbeiter die Veränderungen und sind motiviert ihren eigenen Teil beizutragen. Es folgen nun zwei Beispiele für Probleme, die mit Compliance auftreten können.

Fall 1 Umgehung von Compliance Den Mitarbeitern im Unternehmen wurde die Einführung der Compliance mitgeteilt und es ist bekannt, dass Compliance für das Unternehmen überlebenswichtig ist. Es besteht jedoch die Möglichkeit, dass Compliance dennoch umgangen wird. Grund hierfür können Interessenkonflikte sein, die durch ungünstige Kommunikation des Managements entstanden sind. Fordert das Management beispielsweise höhere Produktivität der Mitarbeiter, so besteht die Möglichkeit, dass die Mitarbeiter Compliance zu Gunsten der Produktivität umgehen[DJHG].

Fall 2: Lähmung durch Compliance Eine weitere Problematik kann entstehen, wenn ein Mitarbeiter ungewollt gegen Compliance-Vorgaben verstößt und das Management darauf unangemessen reagiert. Führt das Mangement beispielsweise als Reaktion auf einen Compliance-Verstoß unhandliche Genehmigungsprozesse ein, so geht die Produktivität der Mitarbeiter zurück. Eventuell werden die Mitarbeiter verunsichert und schlimmstenfalls durch Angst etwas falsch zu machen „gelähmt“[DJHG]. Das Unternehmen geht in einen Stillstand über.

Diese beiden Fälle sollen zeigen, dass es sehr wichtig ist, die Mitarbeiter sinnvoll mit Compliance zu konfrontieren und anstelle von Genehmigungsprozessen mehr auf klare Kommunikation zu setzen.

5 Fazit

IT-Compliance ist aufgrund der wachsenden Menge von IT-Infrastruktur in Unternehmen immer wichtiger, da sie zur Minimierung von Risiken beiträgt und somit Robustheit und Stabilität in das Unternehmen bringt. Die ISO 27001 setzt darauf auf und stellt rückt Datensicherheit in den Mittelpunkt, und ermöglicht dank Zertifizierungen deren Nachweis. Ein zertifiziertes Unternehmen steht so in den Punkten Image, Kredite und Wettbewerb besser da und kann so mehr Kunden gewinnen, die hohe Anforderungen an ihre Dienstleister haben. Abschließend bleibt zu erwähnen, dass Compliance nicht nur eine Frage der Prozesse, sondern eine Frage der Mitarbeiter ist. Somit behält eine klare und postive Kommunikation vom Management immer noch ihre große Wichtigkeit.

6 Literaturverzeichnis

Literatur

Cor. Computer Sciences Corp. CSC-Studie: Wiederherstellung des Gleichgewichts. `http://www.csc.com/de/insights/121737-csc_studie_wiederherstellung_des_gleichgewichts`. Zuletzt abgerufen am: 04.11.2016.

DJHG. Dr. Antonia Steßl Dr. Jan-Hendrik Gnändiger. Im Blickpunkt: Akzeptanz von Compliance Management-Systemen auf Mitarbeiterebene. *Berufspraxis: Compliance*.

ISO13. Information technology - Security techniques - Information security management systems - Requirements. Standard, International Organization for Standardization, Geneva, CH, 2013.

Wika. Wikipedia. Compliance (BWL) — Wikipedia, the free encyclopedia. `https://de.wikipedia.org/wiki/Compliance_(BWL)`. Zuletzt abgerufen am: 03.11.2016.

Wikb. Wikipedia. Compliance Management System — Wikipedia, the free encyclopedia. `https://de.wikipedia.org/wiki/Compliance_Management_System`. Zuletzt abgerufen am: 04.11.2016.

Wikc. Wikipedia. IEC 27001 — Wikipedia, the free encyclopedia. `https://de.wikipedia.org/wiki/ISO/IEC_27001`. Zuletzt abgerufen am: 04.11.2016.

Wikd. Wikipedia. IT-Compliance — Wikipedia, the free encyclopedia. `https://de.wikipedia.org/wiki/IT-Compliance`. Zuletzt abgerufen am: 25.10.2016.

Wike. Wikipedia. IT-Grundschutz-Kataloge — Wikipedia, the free encyclopedia. `https://de.wikipedia.org/wiki/IT-Grundschutz-Kataloge`. Zuletzt abgerufen am: 03.11.2016.