COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/compliant-aus-reinem-selbstschutz,1892243

**Mit Checkliste fürs IT-Management**

# Compliant aus reinem Selbstschutz

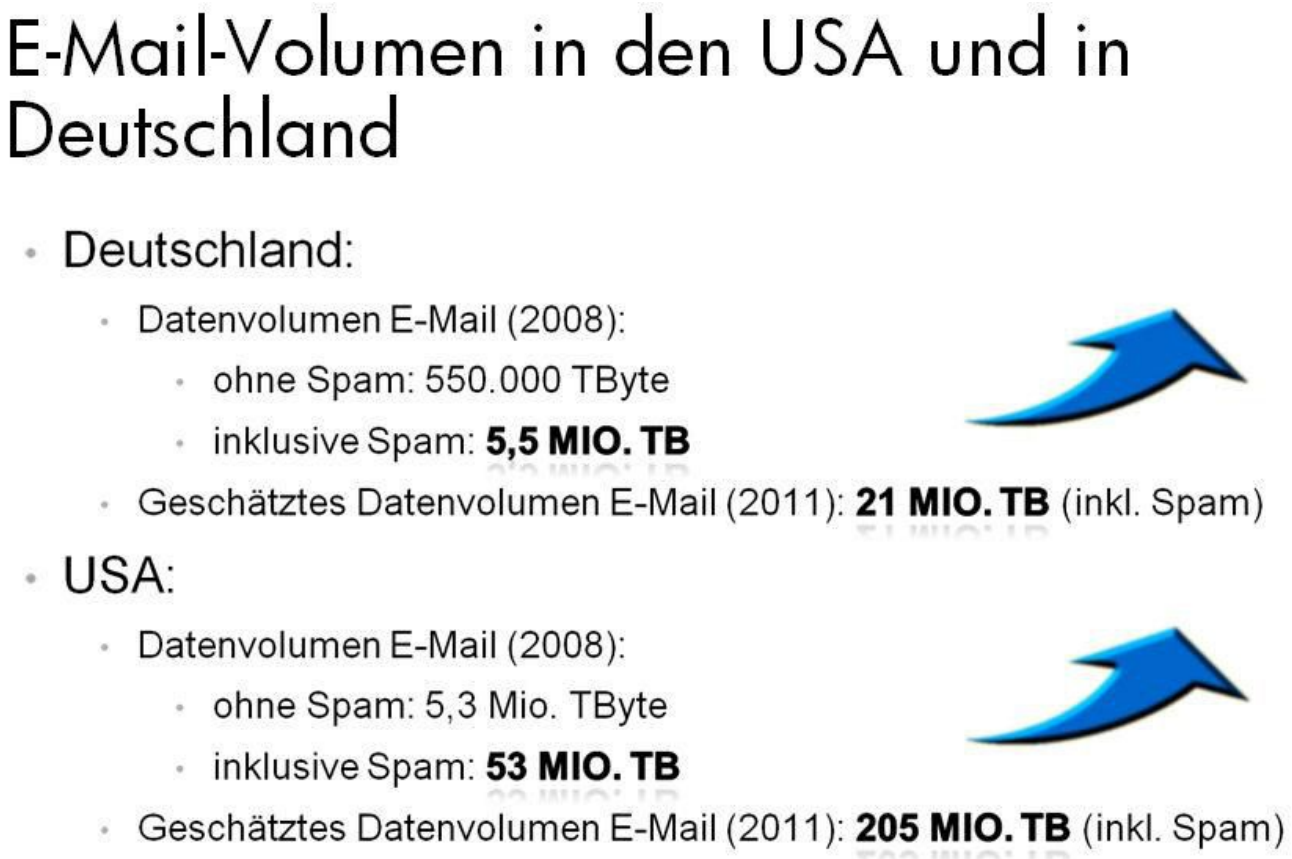
**Datum:** 06.04.2009
**Autor(en):** Johann Baumeister

**Der Begriff "Compliance" weckt Assoziationen mit abstrakten Regelungen und gesetzlichen Vorschriften. Doch die Einhaltung von Regeln und Vorgaben erlebt nicht zuletzt wegen des Finanzdestasters eine Renaissance. Compliance sorgt für Sicherheit der IT und spielt eine bedeutende Rolle zur Absicherung des gesamten Unternehmens gegen Angriffe und Fehler.**


Archivierte Daten müssen zwischen sechs und zehn Jahre aufbewahrt und sämtliche geschäftsrelevanten E-Mails gespeichert werden: Das ist nur ein Bruchteil der Regelungen diverser gesetzlicher Vorschriften.

Der Komplex der **Compliance**[1] wird häufig auf abstrakte Regelungen reduziert. **Basel II**[2], **GdpdU**[3] (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) oder **KonTraG**[4] (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) sind die begleitenden Schlagworte hierzulande. In den USA oder für Unternehmen, die an der US-Börse notiert sind, gehören Begriffe wie **SOX (Sarbanes-Oxley Act)**[5] oder HIPAA (Health Insurance Portability and Accountability Act) zum Compliance-Vokabular.

Der direkte Bezug zum Tagesgeschäft der IT wird nur als gering betrachtet und daher, wenn möglich, eher ignoriert. Gerade in diesen Tagen gewinnen Regeln und Vorgaben allerdings eine enorme Brisanz, wenngleich dabei auch nicht immer das Schlagwort der Compliance fällt. Wenn in den Medien von einer neuen Finanzordnung die Rede ist, geht es im Kern auch immer um Vorschriften der Compliance. **Ethik, Moral, Selbstverpflichtung**[6] oder schlichtweg die Einhaltung von geschrieben oder auch ungeschrieben Regeln bekommt im Rahmen, der aus dem Ruder gelaufenen Finanzgeschäfte, eine neue Bedeutung. Um diese auch umzusetzen bedarf es der erwähnten gesetzlichen Vorgaben und Vorschriften.




Compliance-Vorschriften fordern sogar die Speicherung von Spam, ein enormer Aufwand.

Auch Unternehmen, die sich am Kapitalmarkt finanzieren, müssen heute ihre Projekte und Geschäftstätigkeit genauer nachweisen. Damit deren Geschäfte allerdings von den Geldgebern auch nachvollzogen werden können, müssen allgemeine Regeln zur Bewertung eingehalten werden.

### Jérôme Kerviel von der Société Générale kannte die Systeme aus dem Effeff

Welche enormen Auswirkungen die Missachtung von Unternehmensregeln haben kann, zeigt allein das Beispiel des Wertpapierhändlers Jérôme Kerviel der französischen Bank Société Générale der im vergangenen Jahr unter Umgehung der Unternehmensvorgaben fünf Milliarden Euro verspielt haben soll. Nach Berichten hatte Kerviel einen guten Einblick in die Funktionsweise der Systeme und konnte so die vorhandenen Kontrollen umgehen. In den USA wiederum lieferte vor einigen Jahren der Enron-Skandal die Vorgaben für SOX.

Bricht man diese Vorgaben auf das Tagesgeschäft der IT herunter, so zeigen sich durchaus die Wechselwirkungen. Die Anforderungen an die IT in Fragen der Compliance beschäftigen sich mit den Regulatorien oder gesetzlichen Vorgaben. Dabei geht es häufig um die Frage, wer wann auf welche Daten Zugriff hat oder hatte, wer beispielsweise Daten gelöscht, eingefügt, geändert oder kopiert hatte und wem diese Daten zur Verfügungen gestellt wurden.

### Compliance-Anforderungen an die IT

Bei den Daten in diesem Sinn geht es sowohl um die Inhalte der Datenbanken, aber auch um Dokumente oder Emails und sonstigen Nachrichtenverkehr. Für den IT-Betrieb stellt sich dabei die Frage, wie denn das Unternehmen "im Einklang mit den Regeln und Vorgaben" seine Geschäfte abwickeln kann. Die Antwort darauf liegt zum Einen in der angemessenen Rechtezuweisung und Konfiguration der System und gleichzeitig aber auch der in der Überwachung der Vorgänge.


2002 bekam die Deutsche Bank eine 1,65 Millionen-Strafe aufgebrummt. Der Grund: Fehlerhafte Email-Archivierung.

Allein durch das Wissen über die Überwachung lassen sich viele Übergriffe vermeiden. Dies ist gleichbedeutend mit einer sichtbar angebrachten Überwachungskamera gegen Diebstahl oder Übergriffe. Dabei kommt es nicht so sehr auf die tatsächliche Aufzeichnung der Geschehnisse an, sondern allein die sichtbare Präsenz der Kamera vermag Übergriffe zu verhindern. Daher haben mitunter auch Attrappen, sofern sie als echt betrachtet werden, ein vergleichbar abschreckende Wirkung.

### Auditing-Systeme zur Überwachung der Aktivitäten

Die Überwachungskameras der IT sind die Auditing-Systeme. Sie zeichnen die Geschehnisse minutiös auf und ermöglichen später eine Rekonstruktion der Vorgänge. Die Grundlagen dazu liegen in den überwachten Systemen selbst. Diese protokollieren alle wichtigen Ereignisse in Logbüchern. Hierbei kann es sich um ganz grundsätzliche Betriebssystemaktionen handeln, wie etwa der Anmeldung eines Benutzers oder den Zugriff auf bestimmte Dateien. Daneben stehen die mehr sicherheitsbezogen Ereignisse, wie etwa das Einrichten oder Ändern von Zugriffsrechten. Manche der Softwaresysteme erlauben auch die Definition eigener Ereignisse, die zu protokollieren sind.

Die protokollierten Ereignisse werden dann zur Auswertungen in Protokolldateien hinterlegt. Windows stellt dazu seit mehreren Jahren seine Ereignisanzeige zur Verfügung. In Unix sind es die Syslogs. Die Auswertung der Log-Daten passiert meist nur dann, wenn ein besonderer Bedarf vorliegt. Dazu bedient man sich gängiger Suchalgorithmen.

Die besondere Herausforderung im Umgang mit den Log-Daten liegt aber in der Korrelation der Daten. Erst durch die Verknüpfung unterschiedlicher Informationsmerkmale offenbaren manche Ereignisse ihre Brisanz. So mag beispielsweise der Kauf oder Verkauf von Aktien des eigenen Unternehmens im Prinzip keine Besonderheit darstellen. Fällt er aber mit dem Bekanntwerden von Umsatzänderungen oder wichtigen Kooperationen zusammen, so liegt der Verdacht des Insiderhandles nahe.

## Durch Korrelation der Daten zu besseren Aussagen

Etwas konkreter auf die IT bezogen könnte beispielweise die Anmeldung eines Benutzers, zusammen mit den Änderungen von Dateien oder der Versand von Emails mit kritischen Anhängen außerhalb der Geschäftszeiten auf Datendiebstahl verweisen. Diese Protokollierung der Ereignisse und deren Korrelation ist die Aufgabe des **Compliance Log Warehouse**[7] (CLW) von HP. Dabei handelt es sich um eine Appliance, die ohne aufwändige Konfiguration sehr schnell in Betrieb zu nehmen ist. Einem Data Warehouse gleich sammelt es laufend alle wichtigen Ereignisse ein und stellt diese in Bezug zueinander.

## Trigger und Schwellwerte zur Compliance-Überwachung

Werden Schwellwerte über- oder unterschritten, so generiert das CLW selbständig Alarme oder stößt weitere Aktionen an. Da einfache Schwellwertabweichungen oftmals aber irreführend sind, ermöglicht das Monitoring-Tool auch eine wahlfreie Kombination der überwachten Paramater. So lassen sich beispielsweise die Statusmeldungen einer **Firewall**[8] mit denen eines **Intrusion Detection System**[9] zu besseren Aussagen kombinieren. Um einen umfassenden Überblick zu allen sicherheitsrelevanten Geschehnissen zu gewinnen, ist es notwendig, auch vollständig darüber informiert zu sein.

Daher ist das CLW mit über 180 Adaptoren für alle gängigen Softwaresysteme ausgestattet. Die unterstützte Palette reicht von diversen Betriebssystemen, über Applikationssysteme, Datenbanken bis hin zu den Netzwerkkomponenten wie Firewalls oder IDS. Wenn notwendig, so kann das Unternehmen auch eigene Adaptoren erstellen.

## Echtzeitverarbeitung für Ad hoc-Abwehr

Eingeschlossen ist ferner eine Echtzeitverarbeitung (Real Time Event Correlation) der Ereignisse mit anschließender Alarmierung. Damit lassen sich bei Angriffen oder sonstigen Gefahren unmittelbar Abwehrreaktionen einleiten. Alle Aktionen und Schwellwerte sind durch den Anwender zu bestimmen und können auch nach eigenen Anforderungen justiert werden.

Ebenso wichtig wie die eigentliche Sicherheit und die Einhaltung der Compliance-Vorgaben ist auch dessen Nachweis. Der Analyse und dem Reporting der Compliance kommt daher eine entscheidende Rolle bei. Das Compliance Warehouse umfasst daher eine Vielzahl an unterschiedlichen Berichten zum Nachweis der Compliance. Um auch größte Mengen an Daten zuverlässig verwalten zu können, hat **HP**[10] das CWH auf höchste Leistung getrimmt. Die Skalierbarkeit kommt mit Datenvolumina bis 100 TByte zurecht.

## Gesetztes-konforme Archivierung

Ein weiterer Aspekt der Compliance betrifft die Sicherung der Daten an sich. Diese müssen entsprechend der unterschiedlichen Vorschriften elektronisch archiviert werden. Dabei muss sichergestellt sein, dass die Daten nicht verändert oder gelöscht werden können. Gleichzeitig sollten Daten, für die die Aufbewahrungsfrist abgelaufen ist, auch tatsächlich gelöscht werden. Eine Aufbewahrungsfrist von zehn oder mehr Jahren ist nicht ungewöhnlich.

In dieser Zeitspanne ändern sich in der IT aber häufig die verwendeten Speichertechniken. Daher muss dafür gesorgt werden, dass die Daten auch nach einer längeren Zeitspanne noch lesbar sind. Diese und ähnliche Aspekte adressiert HP in der Integrated Compliant Archiving Solution (iCAS). Dabei handelt es sich um ein Speicherkonzept, dass die oben erwähnten Anforderungen abdeckt. HP iCAS entspricht den rechtlichen Anforderungen für die Archivierung.

Um beispielsweise die Daten vor Veränderung zu schützen werden Hash-Algorithmen, eingesetzt. Desweiteren sorgt die Verschlüsselung der Daten für einen zusätzlichen Schutz. Durch Komprimierung wird der benötigte Platz der Daten eingegrenzt. Als Sicherheit gegen Änderungen oder Löschungen helfen aber auch WORM-Medien.

Ferner lässt sich die Archivierungsdauer für die Daten jeweils spezifisch einstellen. Die Termine werden von der integrierten Software eigenständig überwacht. Die Daten bleiben dabei im Zugriff. Diese kann durch Lastverteilung auch weiter optimiert werden. Das System ist außerdem unabhängig von speziellen Speicherbaugruppen und integriert sich nahtlos in bestehende Speicherinfrastrukturen. Auch die Nutzung bestehender Backup und Replikationslösungen ändern sich durch iCAS nicht. Die Migration von bestehenden Daten von Jukeboxen oder anderen Speichersystemen erfolgt sehr einfach durch Verschieben der Daten auf der Dateiebene.

iCAS ist prinzipiell Unabhängig von der Anwendung. Es eignet sich damit für jegliche Dokumentenmanagement-Systeme, Email-Systeme oder Datenbanken gleichermaßen. Durch eine Datei-System-Schnittstelle erfolgt die Integration mit den Anwendungen.

## Email-Speicherung ohne Verluste

Einen Schritt weiter geht HP bei dem Mail Recorder HP osMR. Das System zeichnet sämtliche eingegangenen Emails auf. Im Gegensatz zum Großteil vergleichbarer Produkt greift HP die Emails aber direkt beim Eingang und noch vor irgendwelchen Spam-Filtern ab. Der HP osMR beruht auf einer Kooperation mit Optimal System. Diese steuern den Mailrecorder bei. Von HP kommt die Archivierungskomponente iCAS.

Aus beiden Bausteinen schnürt HP den HP osMR. In Verbindung mit den Speichersubsystemen von HP entsteht so eine Archivierungslösung die auch den Compliance-Regeln standhält. HP vergleicht den osMR daher auch mit einem Flugdatenschreiber für Emails. Aus rechtlicher Sicht ist dies auch notwendig, weil auch das Entfernen von Emails vor der Archivierung gegen die Compliance-Vorgaben verstößt. Nach einem Urteil des OLG Karlsruhe aus dem Jahre 2005 erfüllt das Löschen und Ausfiltern von E-Mails den Tatbestand des Unterdrückens gemäß § 206 StGB. Daher müssen alle elektronischen Nachrichten archiviert werden. Dies schließt auch SPAM ein.

Das insbesondere die **Speicherung der Emails**[11] eine zentrale Rolle einnimmt zeigen auch ein paar Zahlen zu dessen Nutzung. 35 Milliarden Emails sollen nach einer Prognose des Marktforschungsinstituts IDC weltweit bereits in 2005 täglich versendet worden sein. Für das Jahr 2008 rechnet HP für Deutschland bereits mit 5,5 Millionen TByte an Emailvolumen. 70 Prozent der geschäftskritischen Daten sind bereits heute in den Emails enthalten. Die Email-Nutzung wird somit zu einer tragenden Säule beim IT-Einsatz. Aufgrund von Webangeboten und der vermehrten Nutzung von Email als allgemeine Kommunikationsplattform fliesen mehr und mehr Angebote, Verträge oder Bestellungen über die Mailsysteme. Für den Kontakt mit dem Endverbraucher stellt Mail neben Telefon ohnehin meist die einzige Drehscheibe dar, über die er sich informiert, bestellt oder auch reklamiert. In vielen Geschäftszweigen gehört Email bereits heute zur zentralen Kommunikationsplattform mit dem (potentiellen) Kunden. In rechtlicher Hinsicht besitzen Emails eine identische Bedeutung wie Geschäftsbriefe in Papierform. Ihre Aufbewahrung wird Aufbewahrung somit zum Teil eines Risikomanagements.

## Sicherung der Email-Bestände

Die Archivierung kann im einfachsten Fall durch **Backups**[12] der Mailpostfächer erfolgen. Dies ist jedoch nur in einfachen Szenarien angeraten. Besser ist in jedem Fall eine vorgangsbezogenen Archivierung. In den Quellsystemen (Mailsystem, Dateisystem, etc) sind dabei nur noch Verknüpfungen zum Archivspeicher vorhanden. Ferner erfolgt eine Trennung des Mailheaders vom eigentlichen Mailinhalt und den Anhängen, sowie die singuläre Speicherung (Single Instance Speicherung) bei identischen Anhängen in mehreren Mails. Das Archivierungssystem kümmert sich dann um alle Details der Emailspeicherung. Dazu gehören auch Angaben zu Aufbewahrungsdauer (Retention Period) mit einer automatischen Löschung des Vorgangs beim Ablauf der Aufbewahrungsdauer. Zur Gewährleistung der angemessenen oder gesetzeskonformen Speicherung aller vorgangsbezogenen Informationen sind dann die Archivierungsregeln, -abläufe und -medien entsprechend festzulegen.

## Fazit

Compliance ist kein abstraktes Thema, dass fernab des Tagesgeschäftes der IT reüssiert. Es stellt vielmehr die Grundzüge des Handelns in der IT dar. Compliance liefert dazu ein Rahmenwerk, um das wichtigste Gut der IT, die Daten, vor Missbrauch oder Verlust zu schützen. Auch die derzeitigen Turbulenzen auf den Kapitalmarkt und der wirtschaftlich Einbruch werden nicht ohne weitere Regelungen bleiben. Diese werden die Aspekte der Compliance einmal mehr in den Vordergrund stellen. Die zentrale IT wird daher nicht umhin kommen, die Compliance-Aspekte stärker in allen IT-Prozessen zu verankern und als solche auch herausstellen.

## Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/c/Compliance.html**
[2] **http://de.wikipedia.org/wiki/Basel_II**
[3] **http://de.wikipedia.org/wiki/GDPdU**
[4] **http://de.wikipedia.org/wiki/KonTraG**
[5] **https://www.cio.de/markt/uebersichten/812425/**
[6] **https://www.cio.de/knowledgecenter/rm/847328/index5.html**
[7] **https://www.computerwoche.de/knowledge_center/security/1860396/**
[8] **https://www.computerwoche.de/schwerpunkt/f/Firewall.html**
[9] **https://www.computerwoche.de/knowledge_center/security/1875904/**
[10] **https://www.computerwoche.de/schwerpunkt/h/HP.html**
[11] **https://www.computerwoche.de/knowledge_center/mittelstands_it/1885578/**
[12] **https://www.computerwoche.de/knowledge_center/software_infrastruktur/1890218/**

---