

## Statement of the Month – Novell Consulting

Düsseldorf, im September 2006

### Compliance: Pflicht oder Kür für den IT-Leiter?

**Seit mittlerweile mehreren Jahren geistert der Begriff „Compliance“ durch die Medien. In einem Atemzug werden dabei der Sarbanes-Oxley Act und Basel II als die relevanten Rechtsnormen genannt. Doch fragt man einmal nach, was unter den Begriffen zu verstehen ist, warum sie ein derartiges Medieninteresse finden und welche Auswirkungen sich daraus für die IT-Abteilung ergeben, so erntet man in der Regel Stirnrunzeln oder Achselzucken. Marina Walser, Business Development Manager Security & Identity Management bei Novell untersucht, warum sich mittlerweile jeder IT-Leiter dringend mit IT-Compliance beschäftigen sollte und nimmt diesen die Angst vor dem komplexen Thema:**

Auslöser für die Diskussion rund um den Begriff „Compliance“ war der Sarbanes-Oxley Act (kurz SOX) aus dem Jahr 2002. Das Gesetz wurde damals vom demokratischen Senator Paul S. Sarbanes und dem republikanischen Abgeordneten Michael Oxley unter dem Eindruck der Bilanzskandale in Unternehmen wie Enron und WorldCom im US-Kongress eingebracht. Ziel des Gesetzes ist es, die Unternehmensberichterstattung zu verbessern und das Vertrauen der Anleger in die Richtigkeit der veröffentlichten Finanzdaten wieder herzustellen. Dem Gesetz unterliegen US- und ausländische Unternehmen, die an US-Börsen (NYSE, NASDAQ, etc.) gelistet sind, sowie deren Tochterunternehmen. Das Gesetz trat am 30. Juli 2002 in Kraft. In ihrer Entscheidung am 2. März 2005 gewährte die amerikanische Börsenaufsicht Securities and Exchange Commission (SEC) ausländischen Unternehmen, die an US-Börsen gelistet sind, einen Aufschub von einem Jahr für die Erfüllung insbesondere der Section 404 des Sarbanes-Oxley Acts. Die entsprechenden Anforderungen müssen damit von diesen Unternehmen also erst für Geschäftsjahre erfüllt werden, die nach dem 15. Juli 2006 enden.

Doch gerade dieser Abschnitt 404 ist aus Sicht der Informationstechnologie besonders wichtig. Er besagt in Kurzfassung, dass Unternehmen, die unter den Sarbanes-Oxley Act fallen, nicht nur über interne Kontrollstrukturen und -verfahren für ihre Geschäftsaktivitäten verfügen, sondern deren Wirksamkeit auch belegen müssen. Genau dieser Prozess wird im Englischen mit „Compliance“ bezeichnet. Dazu sind generell alle Geschäftsprozesse zu analysieren und zu dokumentieren, außerdem muss jederzeit der Nachweis erbracht werden können, dass nur berechtigte Personen Zugriff auf die Finanzdaten haben. Darüber hinaus ist sicherzustellen, dass die Finanzdaten nicht manipuliert wurden. Dies kann heute in den meisten Unternehmen nur noch mit IT-Unterstützung umgesetzt werden. Das Gesetz greift damit direkt in die ebenfalls seit einigen Jahren kontrovers diskutierte „Corporate Governance“ von Unternehmen ein. Corporate Governance ist in der Regel ein sehr vielschichtiger Prozess und umfasst obligatorische und freiwillige Maßnahmen, die Einhaltung von Gesetzen und Regelwerken (eben „Compliance“), die Befolgung anerkannter Standards und Empfehlungen sowie die Entwicklung und Befolgung eigener Unternehmensleitlinien. Ein weiterer Aspekt der Corporate Governance liegt in der Ausgestaltung und Implementierung von Leitungs- und Kontrollstrukturen. Also auch hier der Ruf nach Strukturen, die in der Praxis mittlerweile nur noch mit Hilfe der Informationstechnologie aufgebaut und betrieben werden können.

Damit ist die IT-Abteilung in zweierlei Hinsicht gefordert. Zum einen stellt sie die Systeme für die Prozesskontrolle und deren Dokumentation bereit, zum anderen muss sie dafür sorgen, dass ihre eigenen Prozesse hieb- und stichfest sind und den gesetzlichen Auflagen genügen.

In der Praxis geschieht dies zum Beispiel durch Workflow- und Dokumentenmanagement-Software. Die revisionssichere Archivierung von Dokumenten soll gewährleisten, dass diese sogar in einer juristischen Auseinandersetzung Bestand haben. Die IT-Abteilungen der Unternehmen müssen natürlich auch ihre eigenen Prozesse an den Corporate Governance und Compliance-Regelungen ausrichten. Dazu müssen alle IT-Prozesse klar definiert werden, IT-Service-Management auf ITIL-Basis wird zum absoluten Muss für eine effiziente Leistungserbringung, Qualitätsmanagement und das Controlling. Einen wesentlichen Beitrag zur effizienten Umsetzung von Compliance-Anforderungen leistet spezielle Software für das Identitätsmanagement, die sicherstellt, dass nur Berechtigte Zugang zu bestimmten IT-Systemen haben. Diese Berechtigungen können Software-gestützt vergeben und entzogen werden, im Idealfall geschieht dies automatisiert auf Basis der vorgestellten Rolle, die ein Mitarbeiter im Unternehmen hat. Um dann auch nachzuvollziehen, wer zum Beispiel einen Computer benutzt oder auf bestimmte Systeme und Daten zugegriffen hat, werden die An- und Abmeldungen mitprotokolliert. Dieses Protokoll dient als Nachweis dafür, dass das Unternehmen alle Vorschriften eingehalten hat. Wichtig ist darüber hinaus, wer einem Mitarbeiter diesen Zugriff genehmigt hat. Weiterhin muss sichergestellt werden, dass ein Mitarbeiter nicht gleichzeitig mehrere Rollen einnehmen und damit einen Auftrag oder eine Transaktion sowohl beantragen als auch genehmigen kann (segregation of duties).

Was die Umsetzung der SOX-Vorschriften in der Praxis betrifft, gibt es aufgrund der noch neuen Materie derzeit wenig Erfahrungswerte. Als Orientierungshilfe können die Control Objectives for Information and Related Technology (Cobit) dienen, die vom internationalen IT-Prüfer-Verband Information Systems Audit and Control Association (Isaca, [www.isaca.org](http://www.isaca.org)) kostenfrei zur Verfügung gestellt werden.

Tatsache bleibt: Handlungsbedarf ist da. Und wer nun erleichtert feststellt, dass sein Unternehmen nicht unter die Regelungen des Sarbanes-Oxley-Acts fällt, ist leider noch nicht ganz aus dem Schneider. Auch europäische Regelungen wie Basel II oder Solvency II und deutsche Gesetze wie das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG), das bereits seit 1998 in Kraft ist, enthalten ähnliche Vorgaben zum Thema Compliance und Corporate Governance. Bei Verstößen sind teilweise drastische Strafen vorgesehen. So droht der Sarbanes-Oxley-Act nicht nur mit einer zivil-, sondern auch einer strafrechtlichen Verfolgung, der sich nach den Grundsätzen der Gesellschafterhaftung Vorstand und Aufsichtsrat eines Unternehmens zu unterwerfen haben.

Um sich dem Thema zu nähern hilft es, einige grundsätzliche Regeln zu befolgen:

1. Unternehmen brauchen, um regulatorische und gesetzliche Anforderungen effektiv und effizient umsetzen zu können, eine Compliance-Infrastruktur, die abgestimmt ist auf die Risikomanagement-Prozesse des Unternehmens.
2. Insellösungen sind zu vermeiden. Analysen haben ergeben, dass Unternehmen, die für jede regulative Anforderung Insellösungen schaffen, mit durchschnittlich zehnmal höheren Kosten für Compliance-Projekte rechnen müssen.
3. Die eingeführten Systeme müssen Benachrichtigungen in Echtzeit liefern, um auftretende Probleme rechtzeitig zu erkennen und dem Unternehmen die Möglichkeit zu geben, entsprechend gegenzusteuern. Erkannte Abweichungen von z.B. Richtlinien sollten dann sofort definierte Aktionen auslösen. Zusätzlich müssen Ex-Post-Analysen auf Basis archivierter Logs möglich sein, um beispielsweise Audits von Wirtschaftsprüfern jederzeit unterstützen zu können.

4. Compliance-Status-Berichte sollten jederzeit den aktuellen Überblick auf geeignet aggregierter Ebene liefern und als Dashboard für die Unternehmensleitung zur Verfügung stehen. Zusätzlich müssen (Bedenklichkeits-) Berichte automatisch generiert und von den Verantwortlichen die Kenntnisnahme bestätigt werden.
5. Workflows für die Bearbeitung von Compliance-Verletzungen müssen unterstützt werden. Der jeweilige Status der Bearbeitung muß jederzeit nachvollziehbar sein.

Wer Compliance strukturiert und systematisch anpackt, kann das Thema von der Pflicht zur Kür machen und sich dann wieder ruhigen Gewissens den vielen weiteren Anforderungen an die IT stellen.

## Über Novell

Novell, Inc. (Nasdaq: NOVL) ist seit mehr als 20 Jahren im Markt und entwickelt und vertreibt „Software for the Open Enterprise“. Mit offener, Standard-basierter Software unterstützt Novell mehr als 50.000 Unternehmen und Institutionen in 43 Ländern dabei, ihre IT-Umgebungen einfacher und sicherer zu gestalten und zu verwalten sowie besser zu integrieren. Novell Kunden erhalten die Kontrolle über ihre IT-Infrastruktur zurück und senken die Kosten. Dabei werden sie weltweit von 5.000 Novell Mitarbeitern, 5.000 Partnern und technischen Support Centers unterstützt. Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert – Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere, ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter [www.novell.com](http://www.novell.com) oder [www.novell.de](http://www.novell.de).

Weitere Informationen:

Ulrike Beringer  
Manager Public Relations  
Novell GmbH  
Phone +49 (0) 89 206 002 118  
eMail: <mailto:uberinger@novell.com>  
Internet: <http://www.novell.com>

Novell Presseservice  
vibrio Kommunikationsmanagement Dr. Kausch GmbH  
Markus Pflugbeil  
Senior PR Consultant  
Phone +49 (0) 89 32 15 18 62  
Fax +49 (0) 89 3 21 51 77  
eMail: <mailto:markus.pflugbeil@vibrio.de>  
Internet <http://www.vibrio.de>