

Statement of the Month – Novell Consulting

Düsseldorf, im November 2006

Compliance - Konsequenz machbar

Die Marktbeobachter Experton Group haben im Rahmen einer aktuellen Umfrage herausgefunden, dass sich nur 31 Prozent der Unternehmen in Deutschland ausreichend vor Bedrohungen geschützt fühlen. Das ist erschreckend – schließlich schreiben die aktuellen Compliance-Richtlinien vor, dass Bedrohungen erkannt und bewertet werden und die Unternehmen Gegenmaßnahmen ergreifen müssen. Die verschiedenen Richtlinien zu Compliance, mit denen Unternehmen konfrontiert werden, machen sehr deutlich, dass hier Nachholbedarf besteht. Vor allem bei der Umsetzung der regulatorischen Anforderungen hapert es aber noch. Hier fühlen sich die IT-Verantwortlichen nicht selten im Stich gelassen, es fehlen klare Anweisungen. Die vielfältigen neuen Anforderungen wurden in der Vergangenheit teilweise überhastet realisiert, um kurzfristig zum Beispiel die SOX Compliance zu realisieren. Mit dem Ergebnis, dass die entstandenen Insellösungen nicht selten mehr als das Zehnfache an Kosten verschlingen wie eine integrierte Gesamtlösung. Neue IT-Lösungen schaffen hier Abhilfe – sofern diese konsequent und effizient eingesetzt werden. Einige Unternehmen sind schon auf gutem Wege: 38 Prozent der befragten Unternehmen, so die Experton Group, haben bereits Projekte zur Umsetzung der Compliance-Anforderungen mittels Identity und Security Management in Angriff genommen. Umfassendes IT-Risk-Management ist aber noch die Ausnahme. Marina Walser, Director Business Development Identity and Resource Management Solutions von Novell, untersucht, wie Unternehmen eine effiziente und integrierte IT-Lösung für ihre Compliance-Anforderungen realisieren können:

Compliance Regularien verlangen unter anderem, dass Unternehmen protokollieren, wer wann auf was im Unternehmen zugreift, wer wofür berechtigt ist und wer diese Berechtigungen erteilt hat. Der Nachweis erfolgt heute häufig mit erheblichem manuellen Aufwand. Einen zentralisierten und automatisierten Nachweis, quasi auf Knopfdruck, können die wenigsten Unternehmen erbringen. Das stellt die IT vor nicht unerhebliche Herausforderungen, denn wertvolle Ressourcen werden für manuelle, rückwärtsgerichtete Prozesse gebunden und dringend anstehende Business-Projekte können nur verzögert bearbeitet werden. Die unterschiedlichen Richtlinien und Regelungen beinhalten eine Vielzahl unterschiedlicher Kontrollen, wobei die IT meist die folgenden Anforderungen erfüllen soll: Die Zugriffsberechtigungen müssen kontrolliert und verwaltet werden, ein automatisierter Nachweis über Berechtigungen muss erfolgen, Doppelungen bei Nutzer-IDs müssen eliminiert, die Passwort-Vergabe verwaltet und Policies durchgesetzt werden. Zudem sind Maßnahmen zur Vorbeugung gegen nicht autorisierte Zugriffe unerlässlich. Unternehmen müssen außerdem regelmäßige Audits über Zugriffsberechtigungen durchführen. Wichtig ist dabei auch, dass Zugriffsberechtigungen wieder zurückgezogen werden, wenn die Grundlage für den Zugriff nicht mehr besteht. Dies ist zum Beispiel bei einem Wechsel in eine andere Abteilung oder beim Ausscheiden eines Mitarbeiters erforderlich. Diese Regelungen betreffen aber nicht nur die eigenen Mitarbeiter, sondern auch die verschiedensten Gruppen externer Benutzer, wie Berater, Zeitarbeitskräfte, Mitarbeiter von Lieferanten oder Kunden. Und der gesamte Prozess sollte natürlich ohne negative Auswirkungen auf die Geschäftsprozesse erfolgen, das heißt berechtigte Zugriffe dürfen nicht behindert und Prozesse nicht verlangsamt werden.

In drei Schritten zur integrierten IT-Lösung

Um diese Anforderungen effizient umzusetzen, sind drei wesentliche Bereiche zu adressieren: das Zugriffsmanagement, die Sicherheit sowie die Überwachung des Netzwerks.

In einem ersten Schritt kann eine zentrale Verwaltung von Nutzern die Problematik des Zugriffs lösen. So wird an zentraler Stelle der erforderliche Nachweis erbracht. Idealerweise werden die Berechtigungen nicht an Personen, sondern an organisatorische Rollen im Unternehmen gebunden. Grundlage dafür ist natürlich eine Richtlinie zur Definition von Rollen und der Zuordnung von Berechtigungen – diese Voraussetzung muss von den Fachbereichen erfüllt werden, bevor die IT zum Einsatz kommen kann.

Über eine zentrale Passwort-Policy und durch deren Übertragung in alle angeschlossenen Systeme mittels bi-direktionaler Synchronisierung wird die Sicherheit erheblich gesteigert. Äußerst hilfreich ist hier der Ansatz „Single-Sign On“ mit dem nicht nur die Effizienz der Mitarbeiter sondern in erheblichem Maße auch die Sicherheit erhöht wird. Je zahlreicher und je komplexer die benötigten Passwörter sind, umso öfter werden diese notiert – was der Geheimhaltung wenig förderlich ist. Mit nur einer Anmeldung und einem Passwort können somit das Risiko gesenkt und gleichzeitig die erforderlichen Richtlinien umgesetzt werden.

Gegen unberechtigten Zugriff hilft die automatisierte Überwachung aller Ressourcen im Netzwerk. Heute finden sich dort zum Großteil Insellösungen, zum Beispiel für Firewalls, Router oder einzelne Applikationen wie SAP-Systeme. Bei dieser Ausgangslage ist ein Nachweis nur durch manuelles Zusammenführen der Informationen möglich. Die Zusammenhänge zwischen einzelnen Ereignissen bleiben unerkannt. Abhilfe schafft ein zentrales Tool zum „Security Information and Event Monitoring“ (SIEM), das Informationen und Events aus allen Ressourcen im Unternehmensnetzwerk sammelt, diese Daten normalisiert, korreliert, aggregiert und direkt Aktionen zur Behebung auslöst – entweder manuell, teil-automatisiert oder automatisiert. Multiple Dashboards, die auf die Bedürfnisse der jeweiligen Nutzer zugeschnitten sind, optimieren Reporting und Analysen und gewährleisten Transparenz. Um das Dashboard nicht zu überfrachten, ist es wichtig, einen Fokus auf relevante Daten zu setzen. Im Idealfall werden Nutzerverwaltung, Zugriffsmanagement und SIEM verknüpft und über eine zentrale Richtlinie gesteuert. Ein Kreditkarten-Institut setzt zum Beispiel SIEM ein und kann so die Sicherheitsstandards der Payment Card Industry (PCI) effizienter umsetzen. Mit einem automatisierten Audit-Pfad wird der Zugriff auf Daten der Karteninhaber nachverfolgt. Audits lassen sich jetzt deutlich schneller vorbereiten und durchführen. Weitere Vorteile, die sich durch den Einsatz von SIEM über alle Branchen hinweg realisieren lassen, sind die Automatisierung eines Großteils der IT-Kontrollen, erhebliche Produktivitätssteigerungen und die Möglichkeit, ein Vielfaches der Ressourcen effizient zu überwachen.

Die IT stellt also ausreichend Lösungen bereit, um den Ansprüchen von Compliance zu genügen. Gefragt sind jetzt die Entscheider auf Fachseite und in der IT, diese Möglichkeiten zu ergreifen um ihr Unternehmen kostengünstig „compliant“ zu gestalten.

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 4.700 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 oder 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>