

Statement of the Month – Juni 2008

Identity and Security Management

GRC – von der Pflicht zur Kür

Das Wirtschaften im Unternehmen von heute gleicht mehr und mehr einer Simultan-Schachpartie, bei der der Spieler gleichzeitig auf mehreren Brettern unterschiedliche Züge macht. Diese müssen nicht nur nachweislich konform mit den Spielregeln gehen, sondern auch der eigenen Strategie folgen; gleichzeitig birgt jeder Zug ein Risikopotenzial, das genau abgewogen sein will. Um in dieser Situation Herr der Lage zu bleiben, benötigen Unternehmen heute neben Klarheit und Übersicht auch Governance, Risk Management- und Compliance-Tools. Wenn diese drei Tools Hand in Hand arbeiten, dann lassen sich durch sie nicht nur auf Sicherheitsanforderungen von heute reagieren, sondern auch konkrete Geschäftswerte schaffen – meint Marina Walser, Director Identity & Security Management bei Novell Central Europe.

In einer Turnierschachpartie ist der Weg zum Erfolg lang und steinig: Einerseits muss der Spieler darauf achten, dass seine Verteidigung keine Löcher hat; andererseits muss er seine Steine aktiv nach vorne treiben und dabei gewisse Risiken auf sich nehmen. Und nicht zuletzt muss er alle seine Züge dokumentieren und vor dem Schiedsgericht nachweisbar machen, wie es im Einzelnen dazu gekommen ist – selbst wenn sich seine Bedenkzeit bereits zum Ende neigt. Viele Unternehmen erkennen diese Situation wieder: Komplexe Anforderungen, komplizierter werdende Richtlinien und das Schwanken zwischen dem Willen zur Initiative und unkalkulierbaren Risiken kennzeichnen auch die Bedingungen, unter denen sie wirtschaften.

Ein Unternehmer sollte heute wissen, dass er dieses Spiel nicht ohne die Trias Governance, Risk und Compliance gewinnen kann. GRC – damit sind die drei Haupthandlungsebenen eines Unternehmens umrissen: Governance meint die Unternehmensführung durch vordefinierte Richtlinien, also etwa die Festlegung von Unternehmenszielen, die darauf angewandte Methodik zur Umsetzung und die Planung der notwendigen Ressourcen für das Erreichen dieser Ziele. Risikomanagement beschreibt den Umgang von bekannten und unbekanntem Risiken über vordefinierte Risiko-Analysen und deren Management bis hin zu Strategien zur Risiko-Minimierung und dem Vorbereiten von Schadensfall-Puffern bei Risiko-Eintritt. Und Compliance schließlich meint das Einhalten interner wie externer Normen für die Bereitstellung und die Verarbeitung von Informationen, also auch Vorgaben aus Normierungs-Bestrebungen (z.B. Basel II), die Zugriffs-Reglementierung für Daten sowie die gesetzlichen Rahmenbedingungen für deren Verwendung. Umgesetzt werden diese Handlungsebenen einerseits durch intelligentes Management, andererseits durch Softwareunterstützung.

Auf den ersten Blick scheint das gesamte GRC-Thema sehr pflichtbehaftet. Schließlich führt nun mal kein Weg daran vorbei, dass Unternehmen den Nachweis erbringen müssen, gewisse Normen einzuhalten. Aus Sicht des Wirtschaftsprüfers ist eine Sache, die nicht dokumentiert werden kann, einfach nicht existent. Dieses Pflichtprogramm ist aufwändig und schreit geradezu nach passiver Verzettelung. Daher spielen hier auch Software-Werkzeuge eine so wichtige Rolle, die bestimmte Prozesse automatisieren und damit den ungesunden Compliance-Aufwand auf ein erträgliches Maß zurückschrauben. Schließlich kann sich heute kaum ein Unternehmen die Ressourcen leisten, die es kostet, den binnen Jahresfrist wiederkehrenden Compliance-Aufwand stets aufs Neue

aufzurollen.

Software-Werkzeuge helfen dabei gleichermaßen bei den aufdeckenden, wie auch bei den präventiven Kontrollen, wie es im Jargon der Wirtschaftsprüfer heißt. Zum Beispiel kann Identity Management-Software helfen, Log-Files auszuwerten. Damit lässt sich genau nachprüfen, wer wann auf eine bestimmte Datei zugegriffen hat und ob er dazu überhaupt berechtigt war. Und präventiv wirkt Software zum Beispiel durch rollenbasiertes Zugriffsmanagement und damit verbundenen automatischen Genehmigungs-Workflows. Damit kann ein Unternehmen im Voraus sicherstellen, dass nur berechtigte Personen Zugriff auf bestimmte Daten und Anwendungen haben. Auf diese Weise können zum Beispiel die viel zitierten Segregation of Duty-Konflikte ausgeschlossen werden.

Allerdings: Die Aufgabenfelder von GRC sind vielfältig im Unternehmen und das hat in der Vergangenheit dazu geführt, dass viele Unternehmen für unterschiedliche Belange oder Abteilungen unterschiedliche Insellösungen einsetzten. Das wiederum führte einerseits zu kostspieligen Redundanzen, andererseits eröffnet eine solche heterogene Landschaft Sicherheitslücken. Hier ist Abstimmung und Integration der unterschiedlichen Lösungen gefragt und bestenfalls auch eine zentrale Management-Möglichkeit aller GRC-Bereiche.

Um den Wandel zu veranschaulichen: Früher hat sich zum Beispiel die IT-Sicherheitsabteilung im Unternehmen dezidiert mit Themen wie Virenschutz oder Firewalls beschäftigt. Gleichzeitig war eine andere Abteilung für die Rollenvergabe zuständig – beide hatten wenig miteinander zu tun. Heute ist das anders: Rollen-Provisionierung und IT-Security müssen eng zusammenarbeiten. Man stelle sich zum Beispiel vor, ein Mitarbeiter aus der Debitorenabteilung kommt auf die Idee, dass er seine Arbeit effizienter gestalten könnte, wenn er Zugriff auch auf das Kreditorensystem erhält. Also initiiert er den entsprechenden Genehmigungs-Workflow. Der Vorgesetzte sieht aber, dass hier ein Interessenkonflikt besteht und lehnt das Ersuchen aus fachlichen Gründen ab. Jetzt könnte sich der Mitarbeiter an den IT-Administrator wenden, um ihn direkt um die Freigabe der Systeme ersuchen. Weil der IT-Admin mit den fachlichen Gründen nicht vertraut ist, die Argumente des Mitarbeiters aber überzeugend findet, käme er dann eventuell dazu, ihm die Systeme zugänglich zu machen – und damit wäre der Grundstein für einen Konflikt gelegt.

Nur wenn Security und Identity Management zusammenarbeiten, kann eine unter Umständen schädliche Prozessumgehung aufgedeckt werden. Eine integrierte, zentrale GRC-Perspektive würde den Vorfall über die unterschiedlichen Systeme hinweg erkennen und entsprechende Gegenmaßnahmen auf den Weg bringen – also eventuell sofort die Systeme herunterfahren und die letzten Eintragungen im Directory im Kreditorensystem rückgängig machen.

Wenn ein Unternehmen so weit ist, die Bereiche Governance, Risk und Compliance so effizient zusammenzubringen, etwa indem wie im obigen Beispiel die Bereiche Sicherheit und Rollenvergabe integriert sind, dann ist es schon über die reine Pflichterfüllung hinaus. In einem nächsten Schritt kann er nun darauf aufbauend Geschäfts- und Wettbewerbsvorteile aus seiner vorteilhaften GRC-Disposition heraus schaffen – Intern führen Integration und Automatisierung etwa zu effizienteren Geschäftsprozessen; gleichzeitig werden Ressourcen geschont. Und was die Außenwirkung betrifft, so lässt sich durch einerseits integriertes GRC-Denken das Vertrauen und Interesse von Stakeholdern und Kunden beträchtlich erhöhen: Ein Internethändler zum Beispiel, der seine Kundendaten streng nach Compliance-Maßnahmen gesichert hat, um pflichtgemäß bestimmten Normen zu genügen, kann dies auch als vertrauensbildende Maßnahme beim

Kunden ins Felde führen und dadurch unter Umständen etwas anbieten, was der Nächste in der Google-Suchliste nicht hat.

Wenn ein Unternehmen auf dieser Stufe angelangt ist, dann ist es weit über den passiven Umgang mit GRC hinaus. Es ist bereit, die Initiative auf dem Schachbrett des Marktes zu übernehmen.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachusetts (USA), beschäftigt weltweit rund 4.700 Mitarbeiter. 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.

Pressekontakt:

Lars Basche
Text 100 Public Relations
Tel: +49 - (0)89 - 99 83 70-33
E-Mail: novell@text100.de

Ulrike Beringer
Novell GmbH
Tel.: +49 (0)89 20600 2118
Email: uberinger@novell.com