

Statement of the Month – Novell Identity & Security

Düsseldorf im Mai 2007

Spot an – Risiken aus

dass die Anforderungen an ein umfassendes IT-Sicherheitskonzept im Unternehmen in den letzten Jahren deutlich gestiegen sind, hat sich inzwischen herumgesprochen. Das liegt nicht nur an einer allgemein gesteigerten Sensibilität gegenüber Fragen der IT-Sicherheit, sondern vor allem an verschärften gesetzlichen und anderen regulatorischen Rahmenbedingungen. Wurden Umfang und Ausgestaltung interner Kontrollsysteme bislang unternehmensintern definiert, gibt es jetzt genaue Vorgaben, wie beispielsweise KontraG, SOX oder Basel II. Versäumnisse werden teuer, meist haften direkt die Geschäftsführer und Vorstände. Aber wo soll man anfangen? Was entspricht im Unternehmen eigentlich schon der Norm und um welche Norm geht es überhaupt?

Michael Junk, Consultant Identity & Compliance, Novell Central Europe, erläutert, wie Licht ins Dunkel gebracht werden kann.

Vertraulichkeit, Verfügbarkeit und Integrität der Daten nehmen einen immer höheren Stellenwert in jedem einzelnen Unternehmen ein. Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, entsprechende Sicherheitsstandards zu entwickeln und einzuhalten. Insbesondere die Unternehmensleitung muss sich ihrer Verantwortung bewusst werden, denn IT-Sicherheit ist immer Chefsache. Der Sicherheitsprozess muss auf Leitungsebene initiiert und anschließend von allen Beteiligten im Unternehmen mitgetragen und mitgestaltet werden. Verstanden haben das inzwischen viele. Aber ein integriertes und funktionsfähiges Managementsystem für Informationssicherheit (engl.: Information Security Management System, ISMS), das dauerhaft die Informationssicherheit steuert, kontrolliert und Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewährleistet, hat derzeit in den Unternehmen noch Seltenheitswert.

Um transparent zu machen, was bislang fehlt und wie sich die „Lücken“ schließen lassen, bietet sich für Unternehmen jeder Größenordnung eine GAP-Analyse an. Per betriebswirtschaftlicher Definition basiert eine GAP-Analyse auf dem Vergleich zwischen angestrebtem und tatsächlichem Verlauf einer Zielgröße. Wird hierbei eine Lücke identifiziert, dann ist zu überlegen, welches die Ursachen hierfür sind und welche Maßnahmen ergriffen werden sollen, um diese Lücke zu beseitigen.

Auf den Bereich Identity & Security bezogen bedeutet es, das Sicherheitskonzeptes des Unternehmens auf der Basis der ISO-Norm 27001 systematisch zu überprüfen. Diese Analyse kann als Vorbereitung für eine Zertifizierung dienen, ist aber auch für Unternehmen hilfreich, die eine formale Zertifizierung zwar nicht anstreben, die aber ihr IT-Sicherheitskonzept dennoch an dem allgemein anerkannten und von Partnern und Kunden zunehmend erwarteten Stand der Technik ausrichten wollen.

Im Rahmen einer GAP-Analyse werden die IT-Struktur des Ist-Zustandes für relevante Verfahren und Systeme analysiert, die relevanten Systeme auf Basis der Schutzbedarfsfeststellung priorisiert, Risiken analysiert und in Anlehnung an ISO 27001 bewertet, Sicherheitsrichtlinien und interne Kontrollen untersucht, etwaige Lücken im Sicherheitskonzept analysiert und priorisiert und nächste Schritte geplant. Dabei ist es wichtig, die gesetzlichen und regulatorischen Rahmenbedingungen im Auge zu behalten und die Balance zwischen Aufwand und Nutzen von Sicherheitsmaßnahmen zu halten. Die Analyse ist zwar zeitaufwändig, ist aber gut investiert, weil sich die Verantwortlichen anschließend auf die wesentlichen Dinge konzentrieren können.

Der Aufbau eines ISMS orientiert sich dann am sogenannten PDCA-Modell (plan – do – check – act). Von der Erfassung sicherheitsrelevanter Geschäftswerte (assets) über die Identifikation und Einstufung bestehender Risiken bis zur Planung und Umsetzung geeigneter Schutzmaßnahmen erhält das Unternehmen Instrumente zur Kontrolle und Verbesserung der Informationssicherheit innerhalb der Organisation. Das Modell gewährleistet der Unternehmensführung die volle Kontrolle über zu tätige Investitionen und unterstützt das IT-Management dabei, Schwachstellen zu identifizieren und durch den gezielten Einsatz von Mitteln zu beheben. Es ist also nicht ausreichend, dass entsprechende Prozessbeschreibungen (Workflows und Berechtigungen) existieren. Es muss nachvollziehbar dargestellt werden können, dass und wie diese Prozesse funktionieren und ineinander greifen.

Der Aufbau und die Zertifizierung eines ISMS kann die Unternehmenskultur intern wie extern beeinflussen, neue Geschäftsmöglichkeiten mit sicherheitsbewussten Kunden schaffen und zusätzlich die Mitarbeitermoral sowie ihr Bewusstsein für Diskretion am Arbeitsplatz steigern. Darüber hinaus kann so Informationssicherheit durchgesetzt und das Risiko von Unterschlagung, Informationsverlust und unerwünschtem Bekanntwerden der Informationen minimiert werden.

Zuallererst muss die GAP-Analyse aber in den Unternehmen ein Licht anknipsen und die vorhandenen IT-Sicherheitssysteme be- und durchleuchten. Nachschauen und gegebenenfalls aufräumen sowie in Richtung ISMS optimieren, müssen die IT-Verantwortlichen dann noch selbst.

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:

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

Ihre Ansprechpartnerin bei Novell:
Ulrike Beringer
PR Manager Novell Central Europe
Tel: +49 - (0)89 - 206002118
E-Mail: uberinger@novell.com