

## Statement of the Month – Novell Consulting

Düsseldorf, im Oktober 2006

### Mit Trusted Computing zu einer sicheren IT-Umgebung

**Die Sicherheit von IT-Systemen ist ein Thema, das IT-Anbieter wohl nie zur Ruhe kommen lassen wird. Unter dem Stichwort "Trusted Computing" arbeiten die Branchengrößen zum Beispiel seit einiger Zeit daran, eine IT-Infrastruktur zu entwickeln, in der nur so genannte vertrauenswürdige IT-Komponenten (Hard-, Software, Netzwerk) eingesetzt werden. Zudem sollen durch den Einsatz von Verschlüsselungs- und Signaturfunktionalitäten Schadprogramme und Malware ausgeschlossen werden. Das Thema findet breiten Zuspruch: Weltweit sind nach Schätzungen von IDC (Februar 2006, [www.idc.com](http://www.idc.com)) bereits über 50 Millionen Systeme mit Trusted Computing-Technologie ausgestattet. Marina Walser, Director Business Development Identity & Security bei Novell, untersucht die Entwicklung des Trusted Computing-Ansatzes und die Bedeutung für den vertrauenswürdigen Umgang mit Unternehmensdaten:**

Mit der Bedeutung von IT-Systemen für die Abwicklung von Geschäftsabläufen ist auch die Komplexität dieser Systeme stark angestiegen - und damit auch ihre Anfälligkeit für Angriffe von innen wie von außen. Zur Abhilfe wurde im Jahr 1999 die Trusted Computing Group (TCG) gegründet, die mittlerweile mehr als 200 Mitglieder aus allen Bereichen der Informations- und Kommunikationstechnologie (Hardware, Software, mobile Endgeräte, Netzwerkkomponenten) hat. Zunächst ging es hauptsächlich darum, Spezifikationen für vertrauenswürdige und sichere PC- und Server-Systeme zu erarbeiten. Mit der wachsenden Bedeutung von Mobilität werden inzwischen natürlich auch andere Systeme wie PDAs oder Mobiltelefone einbezogen.

Im Rahmen der Spezifikationen der Trusted Computing Group basieren Trusted Computing Systeme im Wesentlichen auf drei Grundbestandteilen: Grundbestandteil Nummer eins ist die so genannte Trusted Platform, eine sichere Rechnerplattform, die in der Lage ist, die elementaren Sicherheitszertifikate und –schlüssel in einer geschützten Hardware-Umgebung zu halten und auszuführen. Dazu enthält sie das so genannte Trusted Platform Module, das wie ein Rechner im Rechner arbeitet und mit umfassenden Sicherheitsfunktionen ausgestattet ist. Der zweite Bestandteil ist die sichere Prozessorarchitektur, die von den großen Prozessorherstellern festgelegt wird und nicht Bestandteil der Standardisierungsarbeit ist. Alle Prozessorhersteller bieten mittlerweile Prozessorgenerationen mit TCG-konformen Sicherheitsarchitekturen an.

Dritter Grundbestandteil des Trusted Computing Systems der TCG sind sichere und vertrauenswürdige Betriebssysteme als Schlüsselemente, um die in Hardware und Prozessoren festgelegten Sicherheitsfunktionen dem Anwender auch zur Verfügung stellen zu können.

Besonderes Augenmerk wird dabei auf den sicheren Zugang zu sowie den Schutz von Unternehmensdaten gelegt. Ein Begriff, der in diesem Zusammenhang immer wieder genannt wird, ist Digital Rights Management (DRM). Im ersten Moment denkt man bei diesem Begriff an den Schutz geistigen Eigentums insbesondere im Zusammenhang mit Raubkopien von DVDs und Softwareprogrammen. Doch genau dieselbe Technik kann auch dazu eingesetzt werden, um das Management von Firmendaten oder die Gestaltung von Dokument- und Workflow-Management-Systemen abzusichern.

Dokumentenmanagement mit DRM verfolgt dabei zwei Ziele: die Rückverfolgung des Absenders eines Dokuments und das Verhindern bzw. Nachverfolgen einer illegalen

Nutzung eines Dokuments. Beispiel Automobilindustrie: Hier entstehen gerade bei der Entwicklung neuer Fahrzeugmodelle zahlreiche patent- und urheberrechtlich geschützte Unterlagen wie technische Blaupausen, Designentwürfe und Skizzen. Diese sollen natürlich vor der Präsentation des neuen Modells geheim bleiben und auf keinen Fall an die Öffentlichkeit, geschweige denn die Wettbewerber gelangen.

Mit entsprechender Workflow- oder Dokumentenmanagement-Software kann sichergestellt werden, dass Mitarbeiter bestimmte Vorgänge, auch wenn sie online passieren, nur gemäß den gültigen DRM-Richtlinien bearbeiten, kopieren und abspeichern. Jeder dieser Vorgänge und Arbeitsschritte wird darüber hinaus protokolliert und kann jederzeit dem entsprechenden Mitarbeiter zugeordnet werden. Geht es darum, die Zugriffsberechtigung eines Mitarbeiters zu kontrollieren oder einzuschränken, kann Software für das Identitätsmanagement dies sicherstellen. Berechtigungen können Software-gestützt vergeben und entzogen werden, was im Idealfall automatisiert auf Basis der voreingestellten Rolle geschieht, die ein Mitarbeiter im Unternehmen hat. Um dann auch nachzuvollziehen, wer den Computer benutzt bzw. auf die Anwendung zugegriffen hat, werden die An- und Abmeldungen mitprotokolliert. Das Unternehmen stellt damit sicher, dass nur berechtigte Personen die Daten öffnen, kopieren oder weiterleiten können. Ein unberechtigter Zugriff wird automatisiert erfasst und mithilfe von Security Event Management Tools wird in kritischen Fällen ein Alarm ausgelöst, der dann umgehend zu Gegenmaßnahmen führt. Identitäts- und Sicherheitsmanagement gehören also zu den tragenden Säulen eines sicheren und vertrauenswürdigen IT-Systems und sollten auf jeden Fall in einer unternehmensweiten Trusted Computing Umgebung implementiert werden.

Bis 2009 erwarten die Analysten, dass etwa 85 Millionen Notebooks, 80 Millionen Server und zirka 75 Millionen Desktop-PCs entsprechende Sicherheitsfunktionen bieten werden. Werden diese Computer mit Lösungen zum sicheren Identitätsmanagement ergänzt, lässt sich damit sichere, gesetztes- und regelkonforme Kommunikation sensibler Informationen durchsetzen.

## 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](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>