

# Datensicherung unterwegs

**Vier Dinge, die jedes Unternehmen unabhängig von seiner Größe bei der Sicherung kritischer Daten auf mobilen Datenverarbeitungssystemen beachten sollte**

Dieses White Paper  
wird präsentiert von



# Datensicherung unterwegs

## Vier Dinge, die jedes Unternehmen unabhängig von seiner Größe bei der Sicherung kritischer Daten auf mobilen Datenverarbeitungssystemen beachten sollte

Von Curtis Franklin, Jr.

### Die Herausforderung: Mobil tätige Mitarbeiter

In der weiten Welt außerhalb Ihres durch Firewalls geschützten Unternehmens gibt es eine wachsende Zahl von Bedrohungen für Ihre vertraulichen Unternehmensdaten. Heutzutage nehmen CEOs und Tischler gleichermaßen ihre Unternehmensnetzwerke mit auf Besuche an Kundenstandorten. Durch dieses neue Maß an Mobilität finden Geschäftsabläufe nun auch verstärkt in der besagten weiten Welt außerhalb der Firmen-Firewalls statt.

Meist sind die auf mobilen Geräten enthalten bzw. über selbige zugänglichen Daten weitaus wertvoller für das jeweilige Unternehmen als das betreffende Notebook, Smartphone oder mobile Gerät selbst. Aus diesem Grund muss jedes Unternehmen eine Datensicherungsstrategie entwickeln, die mobile Szenarien berücksichtigt.

Für KMUs ist die Herausforderung noch größer: Begrenzte Expertise und knappe personelle Ressourcen machen sie besonders anfällig für Gegenspieler, die es mit ihren ausgeklügelten Methoden nicht in erster Linie auf die klassischen Ziele (große Banken etc.) sondern eher auf leichte Beute abgesehen haben. Dieses White Paper beschreibt detailliert die Sicherheitsprobleme, die bei mobilen Datenverarbeitungsgeräten auftreten und erläutert außerdem die Bausteine für die entsprechenden Lösungen.

### Die Gefahren im Detail

Die primären Risiken bei der mobilen Datenverarbeitung lassen sich auf drei verschiedene Arten des unbefugten Datenzugriffs herunterbrechen: Datenverluste, Datenlecks und Datendiebstahl.

**Ein Datenverlust** entsteht durch die ungewollte Freigabe sensibler Daten durch Verlust des Geräts, auf dem die Daten gespeichert sind.

**Ein Datenleck** entsteht durch die gewollte aber nicht autorisierte Freigabe von sensiblen Daten durch die Handlungen eines Mitarbeiters, Vertragspartners oder einer anderen Person mit Zugang zu den internen Unternehmensstrukturen.

**Ein Datendiebstahl** bezeichnet die Aneignung sensibler Daten durch eine außerhalb des Unternehmens stehende Person.

Zusammen genommen stellen diese drei Formen der Datenfreigabe ein beachtliches Risiko für jede Organisation dar – sowohl in finanzieller Hinsicht als auch in Bezug auf die Verletzungen geistiger Eigentumsrechte. Schätzungen zu den wirtschaftlichen Auswirkungen haben einen Schaden von 85 bis 200 \$ pro ungewollt veröffentlichtem Datensatz ergeben. Da in vielen Fällen aber Hunderte bzw. sogar Tausende von Datensätzen betroffen sind, können die Kosten schnell astronomische Größenordnungen annehmen.

Jede mobile Datensicherheitslösung muss, um effektiv zu sein, die im Folgenden beschriebenen vier Elemente beinhalten.

### 1. Richtlinien und Technologien für die Zugriffssteuerung

Um ein Unternehmen vor ungewollter bzw. unberechtigter Datenfreigabe zu schützen, müssen die diesbezüglichen Maßnahmen in den folgenden vier Bereichen koordiniert werden: Mitarbeiter, Richtlinien, Betriebsabläufe und Technologien (zur Umsetzung dieser Richtlinien bzw. Abläufe).

Der Technologieaspekt mag zwar in der Fachliteratur die größte Beachtung finden, steht aber nicht ohne Grund am Ende der Liste: Um effektiv zu sein, muss die Technologie auf praktikablen Richtlinien und Abläufen aufbauen, diese implementieren und außerdem von Mitarbeitern benutzt werden, die sich der Bedeutung der Datensicherheit sowie der Konsequenzen von Sicherheitsmängeln bewusst sind.

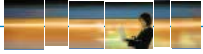
Sicherheit beginnt mit der Zugriffssteuerung. Das Problem der ungewollten Datenfreigabe kann erst in Angriff genommen werden, wenn im Unternehmen klar definiert wurde, welche Personengruppe auf welche Daten zugreifen darf und was sie mit selbigen tun kann. Das wichtigste Puzzlestück bei der Zugriffssteuerung ist also die Entscheidung, wer berechtigt ist, auf welche Daten zuzugreifen. Es mag zwar wie ein unnötiger Zusatzaufwand erscheinen, aber die Erarbeitung von Richtlinien für die Frage, welche Berufsgruppen bestimmte Daten sehen und benutzen dürfen, ist in kleinen Unternehmen ebenso essentiell wie die Anpassung dieser Richtlinien beim späteren Wachstum.

Unternehmenswachstum und Personalveränderungen sind

#### Informationen zum Autor

**Curtis Franklin, Jr.** ist ein auf Technologiethemen spezialisierter Journalist mit einer über zwanzigjährigen Erfahrung in der Computer-, Netzwerk- und Kommunikationsbranche. Innerhalb seiner breit gefächerten journalistischen Tätigkeit hat Curtis Franklin, Jr. sich insbesondere mit den Themen Sicherheit, Mobilität und Netzwerke beschäftigt.

für einen Aspekt bei der Zugriffssteuerung verantwortlich, der sehr oft übersehen wird: die Anpassung der Zugriffsberechtigungen bei Änderung der Berufsgruppe bzw. des persönlichen Aufgabenbereichs. Viele Fälle von ungewollter Datenfreigabe werden durch die Rechte-Situation am betroffenen Account bzw. System zusätzlich verschlimmert. Oftmals sind diese nämlich mit allen Rechten ausgestattet, über die der Inhaber im Laufe seiner Arbeitszeit in der Organisation verfügt hat,



**Sie sollten davon ausgehen, dass nicht dazu**

**berechtigte Personen sich irgendwann einmal Zugang zu Ihren Daten verschaffen werden. In einem solchen Fall sollten die Daten für unautorisiert darauf zugreifende Personen unlesbar bzw. unbrauchbar sein.**

anstatt auf die Berechtigungen seiner gegenwärtigen Position beschränkt zu sein. Wenn die datenbezogenen Zugriffs- und Verwendungsberechtigungen beim Positionswechsel eines Individuums überprüft und angepasst werden, können viele Sicherheitsprobleme von vornherein ausgeschlossen werden.

Nach Erarbeitung und Implementierung zweckmäßiger Richtlinien ist es Aufgabe der Technologie sicherzustellen, dass die Geräte nur von den dazu berechtigten Personen benutzt werden. Bei der Zugriffssteuerung wird meist von einem Stufen- bzw. Faktormodell ausgegangen. Eine zweistufige Authentifizierungsmethode (bzw. Zwei-Faktor-Authentifizierung) stellt dabei ein ausgewogenes Verhältnis zwischen Sicherheit und Benutzerfreundlichkeit dar. In den meisten Fällen handelt es sich bei diesen beiden Stufen zum einen um etwas, das der Nutzer besitzt (z. B. ein System, ein Security-Token oder einen Fingerabdruck) und zum anderen um etwas, das der Nutzer kennt (z. B. ein Kennwort oder eine PIN). Wenn der Nutzer sich bei beiden Stufen korrekt ausweisen kann, gilt seine Identität als überprüft, und der Zugriff auf die Dateien wird gewährt.

Optionen wie naviGo und iCLASS von HID Global ermöglichen in Notebooks von Dell und anderen Herstellern eine Authentifizierung vor dem Bootvorgang. Diese Authentifizierung basiert meist auf Kennworteingabe, Fingerabdruck- oder Smartcard-Scans und erfolgt vor dem Betriebssystemstart, sodass keine Umgehung des Kennwortschutzes möglich ist, um unberechtigterweise auf das System zuzugreifen.

Eines der Hauptprobleme in der Zugriffssteuerung ist heutzutage die Verwendung der "föderierten Identität" bzw. der einmaligen Anmeldung (Single Sign On, SSO). Bei diesen beiden Verfahren wird die Nutzeridentität bei der Erstanmeldung am Notebook oder Smartphone verifiziert und anschließend ohne weitere Prüfung von den benutzten Netzwerken und Anwendungen übernommen. In diesen Fällen muss jedes Unternehmen selbst entscheiden, ob die Zugriffssteuerungsmechanismen an den tragbaren Geräten sicher und zuverlässig genug sind, um als "Pfortner" für das Firmennetzwerk zu fungieren. Eine Reihe von Herstellern bietet mittlerweile leistungsstarke Authentifizierungsmechanismen – wie das SecureID Token-System von RSA – für eine Vielzahl von Geräten an. Diese Lösungen sind durchaus dazu geeignet, einzelnen Unternehmen einen grundlegenden Schutz zu bieten.

## 2. Verschlüsselung

Auch wenn zwischen einer Organisation und ihren Mitarbeitern ein stabiles Vertrauensverhältnis besteht, muss davon ausgegangen werden, dass bestimmte Individuen aus der Belegschaft sich irgendwann unautorisiert Zugriff auf Unternehmensdaten verschaffen. In einem solchen Fall sollten die Daten für unberechtigterweise darauf zugreifende Personen unlesbar bzw. unbrauchbar sein.

Dass die entsprechenden Daten beim Zugriff durch nicht dazu autorisierte Personen für selbige unbrauchbar sind, ist die Aufgabe der Verschlüsselung. Bei der Erarbeitung einer umfassenden Sicherheitsstrategie ist ein Verständnis der Verschlüsselungstechnologie und der Frage, wie und wann sie zu verwenden ist, unabdingbar. In Branchen bzw. Bereichen, wo Vorgaben wie HIPAA oder Massachusetts 201 CMR 17.00 befolgt werden müssen, ist die Verschlüsselung weit mehr als nur eine Option bei der Datensicherung – vielmehr gilt sie dort als eine zuverlässige und obligatorisch einzusetzende Technologie bei Verlust oder Entwendung eines Geräts. In jedem Fall ist es wichtig, zwei grundsätzliche Arten der Verschlüsselung im Datenverarbeitungsbereich zu unterscheiden: die Verschlüsselung von fest an einem Ort befindlichen Daten und die Verschlüsselung von Daten bei der Übertragung selbiger.

Die Verschlüsselung von fest an einem Ort befindlichen Daten beinhaltet die sichere Verschlüsselung des Massenspeichersystems (komplett oder teilweise) des betreffenden mobilen Geräts. Bei der Verschlüsselung der gesamten Festplatte, der so genannten Festplattenverschlüsselung, werden sämtliche Daten auf dem Gerät beim Speichervorgang verschlüsselt und zum Zwecke der Benutzung oder Bearbeitung wieder entschlüsselt. Die Festplattenverschlüsselung hat somit den klaren Vorteil, dass sie eine sichere und einfache Methode für den Benutzer darstellt. Es ist nicht notwendig zu wissen, welcher Teil der Festplatte verschlüsselt ist oder wie man einzelne Dateien verschlüsselt. Der Nachteil liegt im Performance-Bereich, da sämtliche Dateien den zusätzlichen Bearbeitungsschritt der Ver- bzw. Entschlüsselung durchlaufen müssen. In Bezug auf die Sicherheit garantiert die Verschlüsselung der gesamten Festplatte, dass keinerlei Dateien, nicht einmal die unscheinbarsten, durch unberechtigterweise auf das Gerät zugreifende Personen benutzt werden können. Bei der Verschlüsselung einzelner Dateien und Festplattenbereiche besteht natürlich die Gefahr, dass ein Nutzer die betreffende Datei im falschen Verzeichnis speichert, sie nicht verschlüsselt oder einen anders gearteten Fehler begeht, der einen mangelhaften Schutz bedingt.

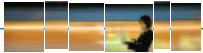
Es gibt eine Reihe Drittanbieterpakete von Firmen wie Wave Systems, PGP, Sophos, GuardianEdge und Credant, die eine Verschlüsselung einzelner Verzeichnisse oder gesamter Festplatten ermöglichen und sowohl auf Windows 7 als auch auf Macintosh OS X Snow Leopard laufen. Smartphones werden normalerweise nicht mit einem zum Betriebssystem gehörenden Geräteverschlüsselungssystem ausgeliefert. Produkte von Firmen wie GP, Navastream und GuardianEdge können aber bei einigen Smartphone-Modellen angewendet werden, um die auf dem Gerät befindlichen Daten zu schützen.

Wenn die an einem Ort befindlichen Daten gesichert sind, kann der nächste Schritt – der häufiger erforderliche Schutz der Daten beim Transport von einem System auf ein anderes – angegangen werden.

VPNs (Virtual Private Networks) werden am häufigsten zur Verschlüsselung beim Datentransport benutzt. VPNs sorgen für eine sichere Verschlüsselung aller Daten, die zwischen zwei Systemen oder Netzwerken unter Benutzung von so genannten Datentunneln verschickt werden. Dazu stehen neben webbasierten SSL-Services (Secure Socket Layer) auch separate Programme zum Aufbau eines IPSec-Tunnels (Internet Protocol Security) unter Verwendung von PPTP (Point to Point Tunneling Protocol) oder L2TP (Layer 2 Tunneling Protocol) zur Verfügung. Im Allgemeinen besteht jede VPN-Verbindung aus zwei Tunneln, die den Datenfluss in beide Richtungen ermöglichen.

Der anfälligste Teil einer VPN-Verbindung ist der Authentifizierungsprozess am Anfang eines Datenaustauschs. Fehler bei der Protokollverwendung können eine unverschlüsselte Versendung der Anmeldedaten bedingen – eine Situation, die Personen mit unlauteren Absichten leicht zum Diebstahl selbiger ausnutzen können. Verschiedene Tunneltypen oder Protokollstapel können gegen die grundlegenden Formen des Diebstahls von Anmeldedaten beim Tunnelaufbau schützen.

Sicherlich kann die Verschlüsselung gegen eine Reihe von Datendiebstahlszenarien schützen. Allerdings müssen die Daten zur Verarbeitung oder Darstellung an einem bestimmten Punkt auch wieder entschlüsselt werden. Dieser Moment stellt eine Schwachstelle dar, die moderne Netzwerk- und Endpunktgeräte-Angriffen zum Diebstahl dieser Daten ausnutzen können.



**Die Abwehr von schädlichen Viren war einst die Hauptaufgabe beim Schutz der auf einem Rechner befindlichen Daten. Heutzutage ist die Virenschutzsoftware nur eine unter vielen wichtigen Sicherheitsanwendungen für mobile Systeme.**

Die Abwehr dieser Angriffe ist Aufgabe spezieller Sicherheitssoftware. Unter Fachleuten wird allerdings zunehmend diskutiert, ob eine Software als Mittel gegen äußerst komplexe und ständig aktualisierte Angriffsmethoden wirklich effektiv sein kann.

### 3. Sicherheitssoftware

Die Abwehr von schädlichen Viren war einst die Hauptaufgabe beim Schutz der auf einem Rechner befindlichen Daten. Heutzutage ist die Virenschutzsoftware nur eine unter vielen wichtigen Sicherheitsanwendungen zum Schutz mobiler Systeme. Software zum Schutz gegen Spam und Adware ist mittlerweile genauso wichtig wie eine Firewall oder eine IDS-Lösung (ein System zum Erkennen von Eindringversuchen und Angriffen). Für viele Organisationen ist die Software zum Schutz gegen webbasierte Bedrohungen genauso wichtig, wie Filter für ein- und ausgehenden Traffic, der als bösartig eingestuft wurde.

Die einzelnen Komponenten können separat bereitgestellt oder aber in einer UTM-Lösung (Unified Threat Management) zusammengeführt werden. Auf diese Weise wird eine Vielzahl von Sicherheitsmechanismen in einem einzelnen Paket kombiniert, um eine umfassendere Abwehr zu ermöglichen.

Da Viren, Würmer, Trojaner und ähnliche Schadsoftware systemspezifisch operieren, war die entsprechende Sicherheitssoftware bisher auch eher systemspezifisch konzipiert. Besonders Microsoft Windows Betriebssysteme dienten den Virenentwicklern in der Vergangenheit als Zielscheibe, weil Computer auf Windows Basis den Großteil des Marktes ausmachten. Als Konsequenz hat Microsoft nun Malware-Schutzsoftware in Windows 7 integriert. Darüber hinaus bieten viele Unternehmen wie Norton, Symantec, CA, F-secure und AVG entsprechende Drittanbietersoftware an. Der Fokus der Malware-Programmierer auf Windows Systeme hat viele Anhänger anderer Systeme zu der Aussage verleitet, dass sie keine Malware-Schutzsoftware benötigen würden. Obwohl die Anzahl der Bedrohungen für Macintosh und Linux basierte Rechner nicht annähernd so hoch ist wie die für Windows Rechner, stellt die Annahme, aus diesem Grund keinen Schutz zu benötigen einen großen Risikofaktor dar.

Um zu beweisen, dass derartige Bedrohungen auch für diese Systeme bestehen, wurden Testviren und -würmer sowohl für Macintosh und Linux Computer als auch für BlackBerry, Palm und Qualcomm Smartphones in Umlauf gebracht. Obwohl tatsächlich sehr wenige für Smartphones entwickelte Viren als im Umlauf bekannt sind, bietet eine Reihe von Unternehmen wie F-secure, Norton, Kaspersky und avast! auch Virenschutzsoftware für diverse Telefone an. Sich beim Systemschutz auf die geringe Verbreitung eines Betriebssystems oder Produkts zu verlassen, ist eine sehr kurzsichtige Herangehensweise, die relativ schnell negative Folgen haben kann.

Malware-Schutzpakete schützen gegen ungewünschte Software, die sich auf dem Computer festsetzen bzw. installieren will. Firewalls hingegen blockieren den Zugriff auf Computer über Netzwerkports, die entweder versehentlich offen gelassen wurden oder aber für die normale Computernutzung gebraucht werden und zum Ziel eines unautorisierten Zugriffs geworden sind. Sowohl Microsoft als auch Apple verfügen über Firewalls in ihren Betriebssystemen. Darüber hinaus werden Firewalls für mobile Computer von einer Reihe verschiedener Hersteller wie Norton, Symantec, ZoneAlarm und Comodo angeboten.

Smartphone-Firewalls sind momentan noch weitaus weniger verbreitet, werden mittlerweile aber auch von Firmen wie Norton, McAfee und Trend Micro vertrieben. Meist werden Firewalls von Systemen zur Erkennung von Eindring- und Angriffsversuchen, den so genannten Intrusion Detection Systems (kurz IDS), ergänzt, die die im System ablaufenden Traffic-Muster und Datenübertragungsvorgänge überprüfen. Wie es der Name schon sagt, beschränken sich viele IDS-Lösungen darauf, den Nutzer bzw. Administrator über ein verdächtiges Muster bei der Datenübertragung zu benachrichtigen. Die Beseitigung der Bedrohung muss dann allerdings der Nutzer selbst oder eine andere Anwendung übernehmen.

Andere IDS-Lösungen können proaktiv gegen verdächtige Datenübertragungsvorgänge vorgehen und Netzwerkverbindungen schließen bzw. die verfügbare Bandbreite drosseln, um die als bösartig eingestuftes Aktivitäten zu verlangsamen oder zu stoppen.

All das hört sich sehr kompliziert und ressourcenintensiv an – und realistisch betrachtet ist es das auch. Die Umfang der vorangegangenen Beschreibungen kann als Erklärung dafür dienen, warum so viele Unternehmen und Individuen nur einen Teil der weiter oben aufgelisteten Sicherheitssoftware implementiert und eine überraschend große Anzahl von Organisationen der Meinung ist, dass ein Schutz überhaupt nicht notwendig sei.

Obwohl die Notwendigkeit von Sicherheitssoftware von den meisten IT-Sicherheitsexperten nicht in Frage gestellt wird, diskutiert man in Fachkreisen sehr wohl ihre Wirksamkeit bei der Abwehr von ausgeklügelten Angriffen. Oftmals geht es einfach nur um das Timing und die Frage, ob die für die Programmsignaturen und Verhaltensmuster der Sicherheitssoftware verantwortlichen Entwickler mit den Kriminellen mithalten können, die ständig nach neuen Wegen suchen, um die Mechanismen eben dieser Software zu umgehen. In der Vergangenheit waren beide Lager meist gleich auf. Das war zum Großteil den Bemühungen unabhängiger Sicherheitsspezialisten zu verdanken, die Probleme sofort nach deren Entdeckung an den Hersteller weitergeleitet haben, damit dieser einen Patch entwickeln und veröffentlichen konnte, bevor die Schwachstelle allgemein bekannt wurde. Heute behauptet ein kleiner aber wichtiger Teil dieser Spezialisten allerdings, dass die Hersteller die von ihnen gelieferten Informationen nicht mit dem nötigen Ernst behandeln. Daher haben sie begonnen, die Details der Schwachstellen fast sofort nach deren Entdeckung zu veröffentlichen, um die Hersteller so zu schnelleren Patches zu zwingen.

Die Konsequenz lautet: Eine Sicherheitssoftware-Paket für mobile Computer ist zwar nach wie vor wichtig, aber nicht mehr länger ausreichend. In modernen IT-Umgebungen ist die Sicherheitssoftware unabdingbar. Sie reduziert den "Security Noise", indem sie die zahlreichen kleineren Eindring- und Angriffsversuche unterbindet, damit sich die Sicherheitsexperten mit den Richtlinien und Überwachungsmechanismen auf die Bekämpfung der ausgeklügelteren Angriffe konzentrieren können. Sachgemäße Verschlüsselung, sichere Authentifizierung, durchdachte Abläufe und effektive Sicherungen sind allesamt ebenso wichtig wie eine leistungsstarke Softwarelösung für die Gesamtsicherheit mobiler Computer.

#### 4. Sicherung

In vielerlei Hinsicht ist die Durchführung von Sicherungen ein vergessenes Element der Datensicherheit auf mobilen Geräten. Werden Sicherungskopien bei Notebooks und Netbooks oftmals einfach vergessen, zieht man sie bei Smartphones meist gar nicht erst in Erwägung. Das kann sich als ein entscheidender Fehler herausstellen, wenn Probleme auftauchen, die einen kompletten Neuaufbau der Betriebsumgebung des betreffenden Geräts erfordern – eine Maßnahme, die häufig zur vollständigen Beseitigung von komplexeren Sicherheitsbedrohungen notwendig ist.

Tatsache ist, dass der Sicherungsprozess auf mobilen Computern einfacher ist als jemals zuvor: Sowohl in Windows 7 als auch in Macintosh Computern wurden Sicherungsanwendungen integriert, des Weiteren stehen Unmengen von entsprechender Drittanbieter-Software zur Verfügung, und für große und kleine Unternehmen sowie Einzelpersonen ist eine Reihe kostengünstiger, cloud-basierter Sicherungsservices erhältlich.

Sogar bei den Smartphones gibt es eine zunehmende Anzahl an Sicherungsoptionen. So verfügt das iPhone innerhalb seines Synchronisationsvorgangs über eine Sicherungsoption und auch für Windows Mobile basierte Smartphones sind Produkte wie Sprite Mobile, PIM Backup und SPB Backup 2 erhältlich. Außerdem bieten DataPilot und andere Hersteller Sicherungssoftware an, die auf einer Vielzahl unterschiedlicher Smartphone-Fabrikate läuft. Der Mangel an Software ist mittlerweile also keine akzeptable Entschuldigung mehr für nicht durchgeführte Sicherungen auf mobilen Geräten.

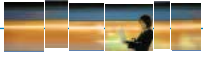
#### Aufbau eines wirksamen Schutzes

Durch die Vielzahl an Schutzoptionen und die Notwendigkeit eines reibungslosen Zusammenspiels unterschiedlicher Lösungspakete hat auch die Integration von Sicherheitssoftware an Bedeutung gewonnen. Systemintegratoren und Hardwareanbietern kommt nun eine wichtige Rolle zu, da sie dafür sorgen müssen, dass

### Dell und die mobile Datensicherheit

**In Dell Geräte werden Daten- und Systemsicherungslösungen integriert, die auf vier Grundpfeilern basieren: Schutz von System und Daten bei gleichzeitiger Verhinderung von unberechtigten Zugriffen und bösartigen Angriffen. Der ControlPoint Security Manager von Dell ermöglicht es den Nutzern, auf einem Notebook die Sicherheitssoftware anderer Anbieter zu aktivieren, zu konfigurieren und deren Status zu überprüfen. Zu diesen Anbietern gehören unter anderem: RSA und HID für die Zugriffssteuerung, Wave Systems für die Festplattenverschlüsselung und Norton oder Symantec Software für den Schutz vor Malware. Zusätzlich unterstützt das ProSupport Laptop Tracking und Recovery System von Dell die Nutzer dabei, verlorene oder gestohlene Notebooks ausfindig zu machen und wieder zu beschaffen. Diese Funktionen können optional mit jedem Dell Latitude und Optiplex Notebook über Dell Business Solutions bestellt werden.**

sämtliche auf einer Plattform laufenden Softwarekomponenten zuverlässig miteinander arbeiten und die Anfangskonfiguration eine sachgemäße Implementierung der kundenseitigen Sicherheitsrichtlinien ermöglicht.



**Die Bestandteile einer Sicherheitslösung müssen für mobile Geräte und Mainframe-Rechner gleichermaßen ein Gleichgewicht zwischen Benutzerfreundlichkeit und effektivem Schutz gewährleisten.**

In letzter Zeit wendet sich eine steigende Anzahl von Kunden mit der Frage nach einer kompletten Sicherheitssoftwarelösung an die Systemanbieter. Damit favorisieren sie den Komfort einer zentralen Anlaufstelle gegenüber der (möglichen) Flexibilität einer selbstständigen Einrichtung ihrer Sicherheitsinfrastruktur. Ganz besonders gilt dies für fast ausschließlich mobil genutzte Geräte, bei denen Remote-Support und -Wartung eher die Regel als die Ausnahme darstellen dürften. Um diesem Bedarf zu entsprechen, kombiniert Dell zum Beispiel die geräteinternen Funktionen von ControlVault (wie den Sicherheitschip, den Fingerabdruck-Scanner und die Authentifizierung vor dem Bootvorgang) mit vorinstallierter Software von Partnern wie RSA, Wave Systems, Seagate und HID Global und bietet so eine einheitliche und umfassende Sicherheitslösung an, die über Dell ControlPoint Security Manager verwaltet werden kann.

Eine zentrale Anlaufstelle, die sowohl die Fragen der Benutzer als auch des Supportdesks beantwortet, vereinfacht nicht nur den komplexen Support der mobilen Unternehmenssicherheit, sondern gewährleistet auch eine schnellere Problemlösung.

### **Schutz, mit dem man arbeiten kann**

Die zunehmende Nutzung mobiler Geräte hängt in großem Maße mit der gesteigerten Bedeutung der Aspekte Mitarbeiterproduktivität und Benutzerfreundlichkeit zusammen. Die Bestandteile einer Sicherheitslösung müssen für mobile Geräte und Mainframe-Rechner gleichermaßen ein Gleichgewicht zwischen Benutzerfreundlichkeit und effektivem Schutz gewährleisten. Bei mobilen Geräten ist dieses Gleichgewicht aufgrund des besonderen Charakters dieser Systeme noch wichtiger: Ein mobiles System mit geringer Benutzerfreundlichkeit wird vom Benutzer entweder gegen ein anderes (möglicherweise weniger sicheres) System ausgetauscht oder aber in Bezug auf die Sicherheitseinstellungen so sehr zu Gunsten der Benutzerfreundlichkeit verändert, dass das IT-Team wenig erbaut darüber wäre.

Die Schulung der mobil tätigen Mitarbeiter hinsichtlich der Bedeutung von Sicherheitsfragen, die Entwicklung durchdachter Richtlinien und Abläufe für die sichere Verwendung von Systemen und Daten sowie die Bereitstellung der erforderlichen Technologien zur Implementierung solider Vorgaben garantieren eine rundum perfekte Sicherheit der Unternehmensdaten – egal, wie weit das entsprechende Gerät auch reisen mag. ★

## Über Dell

**Dell Inc. geht auf die Anforderungen von Kunden ein und bietet ihnen die innovativen Technologien und Services, die sie schätzen. Dell ist ein führender globaler Anbieter von Systemen und Services und dank seines Direktverkaufsmodells auf Platz 33 der Fortune 500 Unternehmen. Weitere Information finden Sie unter [www.dell.com](http://www.dell.com) oder direkt über einen der zahlreichen Online-Channels unter <http://www.dell.com/conversations>. Neueste Nachrichten von Dell erhalten Sie über <http://www.dell.com/RSS>.**