

# Sommer, Sonne, Sorglosigkeit? - Mobiles Arbeit birgt Risiken

**Endlich ist der Sommer nach langer Flaute da. Umso wichtiger ist es, jeden Sonnenstrahl und jeden warmen Tag auch wirklich auszunutzen. Und das ist, dank findiger IT- Unternehmen und plakativer Initiativen wie zum Beispiel „Laptop und Lederhose“ heute ganz einfach. Zahlreiche Biergärten und Kneipen mit Freiluftambiente bieten kostengünstige Wireless-Verbindungen an. So lässt sich die ausgedehnte Mittagspause bequem zum Arbeiten nutzen. Selbst der Zugriff auf sensible Unternehmensdaten ist via VPN kein Problem. Einziges Hindernis ist die Laufzeit des Akkus - oder ein Gewitter.**

Das freut den Mitarbeiter, der dadurch mehr vom Sommer hat, und eigentlich sollte es auch den Arbeitgeber freuen. Schließlich arbeitet der Sonnenhungrige nebenbei, anstatt nur einfach den Sommer zu genießen. Aber die Freude sollte sich eher in Grenzen halten. Denn was passiert, wenn die Apfelschorle alle ist und der moderne Arbeiter seinen Laptop nur einen Moment unbeaufsichtigt lässt? Welche Datenmenge kann jemand in einer Minute auf einen USB-Stick laden – bei der Kapazität und Übertragungsgeschwindigkeit moderner Sticks? Und weder der Anwender, noch die IT-Abteilung werden jemals bemerken, dass Daten kopiert wurden.

Der Freiluftarbeiter kann entgegnen, dass es kaum verlässliche Aufstellungen gibt, was sensible Unternehmensdaten eigentlich wert sind und was sich nicht beziffern lässt, kann so groß nicht sein. Falsch, denn wie viele Mitarbeiter eines Unternehmens erzeugen als Ergebnis ihrer Tätigkeit primär Daten? Nicht selten gilt das für die Mehrzahl. Allein die Summe der Gehaltskosten dieser Mitarbeiter gibt einen guten Einblick, wie viel ein Unternehmen in seine Daten investiert hat. Dazu kommen noch der „Nutzwert“ und der Imageverlust, wenn sensible Daten an die Öffentlichkeit geraten. Da kommt eine erkleckliche Summe zusammen. Zum Großteil befinden sich diese kostbaren Daten auf einem zentralen Server, wo sie bestens abgesichert sind über Gebäudesicherheit und Software-Lösungen wie Firewalls oder rollen-basierte Zugriffskontrollen. Doch der Schein trügt. Denn wer arbeitet mit den Daten? Der einzelne Anwender. Und das ist das Problem.

Egal ob Wireless-Anbindung im Biergarten oder einfach eine Geschäftsreise. Die Frage wo sich jeder Anwender zu einem bestimmten Zeitpunkt geografisch aufhält, können wir in vielen Fällen nicht mehr beantworten, der Mobilität sind keine Grenzen gesetzt. Er mag tatsächlich an seinem Arbeitsplatz sitzen, oder er befindet sich einem Besprechungsraum in einer der Niederlassungen oder aber auch bei einem Kunden, in einem Zug, einem Hotelzimmer oder an einem Flughafen. Und dabei führt er eine viele sensible Daten mit sich. Das äußerste Ende des Netzwerkes eines Unternehmens könnte also in diesem Moment gerade im Seehaus im Englischen Garten in

München oder aber in der Airport Lounge des Flughafen Charles de Gaulles bei Paris sein. Weitab von jeglicher Gebäudesicherheit und allen Firewalls des Rechenzentrums.

Oftmals wird ins Feld geführt, dass einfach beide Seiten Kompromisse machen müssen – der Mitarbeiter bei der Mobilität und das Unternehmen bei den Anforderungen an die Datensicherheit. Aber wie viele Schadensfälle der letzten Zeit beweisen, ist das keine Lösung. Die Erkenntnis, dass überhaupt Gefahren lauern, wenn Mitarbeiter mobil arbeiten, fehlt noch in vielen Unternehmen. Firewalls, Zugriffsbeschränkungen, Verschlüsselungen und viele andere IT-Lösungen schützen fast alle Zu- und Ausgänge zu Unternehmensnetzwerken, aber die Endgeräte, die – meist ohne Transparenz und Kontrolle - mit allen PCs kommunizieren können, sind die Schwachstellen der Unternehmenssicherheit. Moderne Software kann dieses Dilemma beheben: Durch die Implementierung und Überwachung intelligenter Sicherheitsrichtlinien werden Kommunikationsschnittstellen gesichert und Ereignisse erkannt, die auf einen versuchten Datendiebstahl hinweisen. Datensicherheit ist damit jederzeit und an jedem Ort gewährleistet ohne dabei die Produktivität des Anwenders zu beeinträchtigen. Der neugierige Nachbar im Biergarten kann dann zum Beispiel mit seinem USB-Stick wenig ausrichten. Und dem mittagspäischen Arbeiten mit Laptop und Lederhose – oder im Anzug – steht nichts mehr im Wege.

Zwei weitere Statements folgen später diesen Monat und im September und behandeln die Reduzierung von Kosten und Komplexität. Bleiben Sie dran!

Einen schönen und sicheren Sommer wünscht Christoph Stoica, Director End User Computing, Novell Area Central

## **Über Novell:**

Novell, Inc. (Nasdaq: NOVL) bietet eine Linux-Plattform, die für die nahtlose Integration in verschiedenste Plattform- und Anwendungsumgebungen konzipiert ist, sowie ein Portfolio an integrierter IT-Management-Software, mit der Unternehmen weltweit Kosten, Komplexität und Risiken reduzieren können. Mit dieser Infrastruktur-Software und einem umfassenden Partnernetzwerk verbindet Novell heterogene IT-Umgebungen und ermöglicht so, dass Menschen und Technologie als eine Einheit zusammenarbeiten. Weitere Informationen unter [www.novell.com](http://www.novell.com).

## **Pressekontakt**

Ulrike Beringer

Novell GmbH

Telefon: +49 (0) 89 / 28 673 850

eMail: [uberinger@novell.com](mailto:uberinger@novell.com)

Saskia Stolper

Hotwire

Telefon: +49 (0) 69 / 25 66 93-50

eMail: [saskia.stolper@hotwirepr.com](mailto:saskia.stolper@hotwirepr.com)