

Warum in die Ferne schweifen ...

Allerorts wird behauptet, mobiles Arbeiten habe sich in Unternehmen fest etabliert – die Technologie dafür gibt es in der Tat. Wie sieht es in Wirklichkeit aber aus?





Mobiles Arbeiten ist im Kommen. Lange Zeit als Privileg einiger weniger Auserwählter angesehen – Mitarbeiter, die sich der unmittelbaren Kontrolle ihrer Vorgesetzten entziehen durften, galten als überaus wichtig für das Unternehmen –, wird es allmählich

für immer mehr Beschäftigte zur Selbstverständlichkeit: So lautet zumindest die Meinung vieler Marktbeobachter, Berater und Analysten, vor allem der IT-Branche.

Keine Frage: Die technischen Mittel sind vorhanden und, auch wenn sie noch einige Schwächen aufweisen, sie reifen weiter aus, sodass die Arbeit von unterwegs immer besser funktioniert. Schnelle Übertragungstech-

nologien (siehe Kasten auf Seite 54) und ein breites Spektrum an verschiedenen Endgeräten stehen zur Wahl, um sämtliche Arbeitsabläufe mobil zu gestalten. Dabei werden sowohl die Verbindungsgeschwindigkeiten als auch die Reichweite der Breitbandnetze immer höher. UMTS- und Wireless-Technologie machen einen schnellen Zugriff auf das Telefonnetz, das Intranet oder das Internet >

› sowie auf E-Mails und Daten jeglicher Art von jedem Ort und zu jeder Zeit möglich. In Hotels, in Cafés sowie auf Flughäfen und Bahnhöfen – sogar in den Zügen – stehen Hotspots für den Zugang zum Internet zur Verfügung und erlauben es, die unvermeidbaren Wartezeiten produktiver zu gestalten.

Und doch bedienen sich viele Unternehmen dieser Arbeitsform weiterhin nicht. „Mobiles Arbeiten scheint in Deutschland immer noch eine Seltenheit“, schrieb die Financial Times Deutschland Ende 2011 und stützte sich dabei auf eine Online-Blitzumfrage des Kommunikationssystemanbieters LifeSize. Dieser Untersuchung nach sei die Mehrheit der Arbeitnehmer gar nicht oder weniger als einmal im Monat außerhalb des Büros tätig. Diese Ergebnisse bestätigt eine Befragung des Web-Collaboration-Tool-Anbieters Citrix Online, einer Tochtergesellschaft von Citrix Systems. Bereits einige Zeit zuvor hatte das Unternehmen herausgefunden, dass der Anteil der mobilen Arbeit gerade mal für ein Viertel der Beschäftigten in den vergangenen Jahren gestiegen ist, was angesichts der technischen Möglichkeiten eher überraschend sei.



Eine neue Studie – ebenfalls im Auftrag von Citrix Systems von den Marktforschungsunternehmen YouGov und Research Now zwischen Mai und August 2011 unter mehr als 1.100 Senior Executives und IT-Managern in Australien, Frankreich, Deutschland, Großbritannien und den USA

durchgeführt – kam erneut zu dem Ergebnis, dass Unternehmen nicht auf mobiles Arbeiten vorbereitet sind.

Der Grund für diese Zurückhaltung seien Vorschriften der Unternehmen, die einen externen Zugriff untersagen, oder technische Hürden, kommentiert die FTD die LifeSize-Umfrage. „Konkret heißt das häufig, in den Firmen fehlen Sicherheitsvorkehrungen und geeignete Software, die einen geschützten Datenaustausch ermöglichen. Auch die Auswahl der passenden Hardware für mobiles Arbeiten bereitet manchem Manager noch so viel Kopfzerbrechen, dass letztlich oft darauf verzichtet wird.“

IT-CHAOS

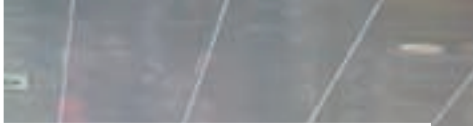
Tatsächlich sieht es in der Praxis häufig so aus, dass sich mobile Arbeiter mit unzureichenden oder gar schlechten Leistungen der benutzten Anwendungen herumplagen und sich infolgedessen vehement bei den zuständigen IT-Kollegen beschweren. Der Grund: Die durch die Pflege der immer zahlreicher werdenden Systeme und Applikationen überlasteten IT-Abteilungen schaffen es nicht, das reibungslose Funktionieren aller Anwendungen zu sichern. So herrscht zunächst Chaos, dort wo eigentlich eine Verbesserung der Geschäftsabläufe eintreten sollte.

„Damit sie ihre Tätigkeit von unterwegs mit der gleichen Effizienz wie am Arbeitsplatz ›

„Damit sie ihre Tätigkeit von unterwegs mit der gleichen Effizienz wie am Arbeitsplatz verrichten können, sind mobile Arbeiter darauf angewiesen, von jedem beliebigen Ort und mit jedem beliebigen Endgerät auf die benötigten Systeme und Informationen problemlos zugreifen zu können.“

DR. MICHAEL DUHME,
Pressesprecher der windream GmbH





CHECKLISTE WLAN-Hotspots sicher nutzen

Öffentliche WLAN-Hotspots leisten gute Dienste. Sie machen es Außendienstlern und anderen mobilen Mitarbeitern möglich, in Flughäfen, Bahnhöfen, Restaurants oder Hotels mittels Notebooks und ähnlicher mit einem Wireless-Adapter (WLAN-Karte) ausgestatteter Geräte, eine Internetverbindung zu erstellen. Um sie sicher zu nutzen, empfiehlt es sich allerdings, einige Punkte unbedingt zu berücksichtigen.

- Zunächst ist es ratsam, ein Benutzerkonto mit eingeschränktem Zugriff zu benutzen. Erweiterte Rechte, wie sie beispielsweise ein Administrator besitzt, haben im Falle eines kriminellen Angriffs auf das mobile Gerät größere Schäden zur Folge.
- Der Hotspot-Nutzer tut ebenfalls gut daran, die Datei- und Verzeichnisfreigabe für Netzwerke zu deaktivieren. Somit haben die übrigen Rechner im WLAN-Funkbereich keine Zugriffsmöglichkeit mehr auf seine Festplatte oder andere Datenträger. Lediglich das TCP/IP (Transmission Control Protocol / Internet Protocol) wird für die Internetverbindung gebraucht. Weitere, überflüssige Netzwerkprotokolle sollte der Administrator unbedingt deaktivieren.
- Überaus wichtig ist es zudem, dass die Software, vor allem Webbrowser, Mail-Client und Betriebssystem, stets mit aktuellen Sicherheitsupdates versehen ist. Dies gilt ebenfalls für die Antivirensoftware.
- Auf Nummer sicher gehen mobile Arbeiter, wenn sie eine Personal-Firewall-Software verwenden. Sie überwacht die Kommunikation zwischen dem Rechner und der Außenwelt. Die Verbindung zum Firmennetzwerk schützt ein Virtual Private Network (VPN), das die Daten zwischen zwei Rechnern über einen sicheren Kanal verschickt. Vertrauliche Daten werden ausschließlich über eine mittels SSL (Secure Socket Layer) gesicherte Verbindung aufgerufen.
- Und um nicht unnötigerweise Angriffsmöglichkeiten zu bieten, deaktiviert der Notebook-Besitzer die WLAN-Komponenten, sobald er den WLAN-Zugriff nicht mehr braucht.

› verrichten können, sind mobile Arbeiter darauf angewiesen, von jedem beliebigen Ort und mit jedem beliebigen Endgerät auf die benötigten Systeme und Informationen problemlos zugreifen zu können“, erläutert Dr. Michael Duhme, Pressesprecher beim ECM-Anbieter windream. „Zentralisierte ITK-Architekturen garantieren den Anwendern den Echtzeitzugriff auf Daten und Applikationen und erlauben es, verschiedene Systeme und Anwendungen unter ein Dach zu bringen.“ Und im Gegensatz zu wild-

wüchsigen und heterogenen IT-Strukturen lassen sie sich zudem ohne großen Aufwand und mit reduzierten Betriebskosten pflegen und administrieren. Der Einsatz von Virtualisierungs-Technologien kann deutliche Vorteile schaffen: Nicht nur, dass er es möglich macht, die IT-Ressourcen besser aufzuteilen; er stellt Server- oder Desktop-Applikationen ohne örtliche Installation zur Verfügung.

Hinzu kommt ein Aspekt, der zu oft in Vergessenheit gerät: die Sicherheit. Bedau-

erlicherweise gehen sowohl Unternehmen als auch ihre Beschäftigten mit dem Thema immer noch überaus sorglos um. Dabei sollte der Zugriff auf die Firmennetze nicht nur verlässlich, sondern auch sicher sein. Fakt ist aber, dass die Nutzung von mobilen Endgeräten für den Zugang zu unternehmenskritischen Anwendungen ein großes Risiko darstellt. Daher will ihre Integration in die IT-Infrastruktur gut überlegt sein: Die Endgeräte und die Kommunikation mit dem Unternehmensnetz bedürfen der gleichen ›

› Absicherung wie Systeme und Zugänge im lokalen Netz.

Schwierigkeiten bereitet dabei die Vielfalt der Geräte und der Kommunikationstechnologien. Notebooks oder Tablet-PCs, die sich per WLAN über öffentliche Hotspots ins Unternehmensnetz einbinden, brauchen die gleiche Unterstützung wie PDAs oder Smartphones, die mit unterschiedlichen Systemen laufen und mobile Datendienste wie GPRS (General Packet Radio Service) oder UMTS (Universal Mobile Telecommunication System) nutzen. Hinzu kommt, dass Mitarbeiter unterwegs immer öfter ihr privates System benutzen und die Sicherheitsverantwortlichen keinen Zugriff darauf haben. Klar, dass sich da Virenschreibern und anderen Hackern viele Angriffswege bieten.

So zeigt etwa die jüngste, bereits erwähnte Citrix-Systems-Studie, dass gerade kleine und mittelständische Unternehmen (KMU) zunehmend dem Druck ausgesetzt sind, ihren Mitarbeitern den Einsatz von privaten Smartphones, Tablets und anderen Geräten auch im Arbeitsalltag zu ermöglichen. Ein Viertel der befragten Unternehmen unterstützt den Einsatz am Arbeitsplatz bereits, viele von ihnen profitieren dabei von erheblichen Produktivitätssteigerungen um 30 Prozent, da ihre Mitarbeiter nun von überall und jedem Gerät aus ihrer Arbeit nachgehen können. Die Bereiche Sicherheit und Vertraulichkeit der Daten kommen jedoch häufig noch zu kurz: So verfügen 62 Prozent der Unternehmen über keinerlei Regeln und Prozesse, die den

Einsatz von privaten Endgeräten kontrollierbar machen. 45 Prozent der IT-Manager haben darüber hinaus keinen Überblick über alle Geräte, die von den Mitarbeitern für berufliche Zwecke eingesetzt werden.

„Unsere Umfrage zeigt, dass Mitarbeiter ihre privaten Endgeräte zunehmend auch beruflich einsetzen“, berichtet Robert Gratzl,

Vice President und General Manager EMEA von Citrix Online Services Division. „Unternehmen müssen auf diese Entwicklung mit adäquaten Regeln reagieren, um den sicheren Umgang mit sensiblen Unternehmensinformationen zu gewährleisten. Dadurch ergibt sich die Chance, ihre Produktivität durch flexiblere Arbeitsmodelle zu steigern.“

INFO

Unterschiedliche Übertragungstechnologien erlauben es mobilen Anwendern von Laptops, Netbooks oder Handys, online zu gehen wann und wo sie wollen. Verschiedene Netze und Geschwindigkeiten stehen ihnen zur Verfügung und sichern ein Höchstmaß an Flexibilität. Auch der Wechsel von einem Netz zum anderen gestaltet sich als unkompliziert.

GPRS (GENERAL PACKAGE RADIO SERVICE)

Während der Datenübertragung werden die Informationen in einzelne Datenpakete zerlegt und beim Empfänger erneut zusammengesetzt.

Vorteil: GPRS steht in Deutschland fast flächendeckend zur Verfügung. Auch in abgelegenen Gebieten erweisen sich Empfang und Sprachqualität als sehr gut. GPRS ermöglicht eine Abrechnung nach Volumen. So kann der Anwender immer online sein, ohne dass zusätzliche Kosten anfallen.

Nachteil: Mit einer Datenübertragungsgeschwindigkeit von bis zu 55,6 kbit/s bietet GPRS eine ähnliche Leistung wie analoge Modems im Festnetzbereich.

EDGE (ENHANCED DATA RATES FOR GSM EVOLUTION)

Breitbandanschluss zum Herunterladen von Bildern und großen Dateien. EDGE ist schneller als GPRS: Im Download sind Datenübertragungsraten um die 230 kbit/s möglich. Im Upload werden immerhin noch um die 110 kbit/s erreicht.

Vorteil: EDGE stellt den breitbandigen, flächendeckenden Zugang zum mobilen Internet sicher.

UMTS (UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM)

UMTS ist der Mobilfunkstandard der dritten Generation.

Vorteil: Die Technologie ermöglicht Übertragungsgeschwindigkeiten von bis zu 384 kbit/s.

Nachteil: UMTS ist nicht flächendeckend verfügbar.

Wer ein noch höheres Tempo möchte, braucht **HSDPA (HIGH SPEED DOWNLINK PACKET ACCESS)**. Beim Datenempfang erreicht die Weiterentwicklung von UMTS eine maximale Übertragungsgeschwindigkeit von bis zu 7,2 Mbit/s. Und auch beim Hochladen schafft HSUPA (High Speed Uplink Packet Access) bis zu 3,6 Mbit/s.

WLAN (WIRELESS LOCAL AREA NETWORK) steht an Bahnhöfen, Flughäfen, in Hotels, Cafés und in manchen Zügen zur Verfügung. In Deutschland gibt es inzwischen mehr als 15.000 WLAN-Hotspots. Je nach Netzauslastung ist eine Übertragungsgeschwindigkeit von bis zu 11 Mbit/s möglich.



Um die durch die Nutzung von Privatgeräten entstehenden Gefahren in Schach zu halten, erweisen sich ausführliche Schutzmaßnahmen als unverzichtbar. Damit sind nicht nur die Absicherung der Systeme und des Zugangs zu Unternehmensdaten, sondern ebenfalls organisatorische Maßnahmen gemeint. Die Unternehmen und ihre IT-Administratoren sind gut beraten, Sicherheitsrichtlinien für die Mitarbeiter sowie Regeln für das Management der Geräte zu definieren und konsequenterweise für ihre Einhaltung zu sorgen.

STRENGE REGELN

Diese Richtlinien oder sogenannten Policies für Notebooks, WLAN-Netze, PDAs und Handys müssen ein paar wichtige Aspekte regeln. Vor allem sollten sie feststellen, welche mobilen Geräte die Mitarbeiter für den Zugriff auf Unternehmensanwendungen benutzen dürfen. Die Absicherung gegen unerwünschten Zugriff ist umso einfacher und effektiver, je weniger mobile Plattformen und Technologie verwaltet werden müssen.

Wichtig: Die Geräte sollte ausschließlich die IT-Abteilung konfigurieren. Auch sollte sie so wenig Anwendern wie möglich Zugriffsrechte erteilen, und dies ohne Ausnahme, wie etwa für leitende Mitarbeiter.

Daten können aber auch auf noch einfachere Weise als durch kriminelle Angriffe in

„Gegen das Risiko durch Malware helfen nur eine aktuelle Schutzsoftware und die Aufklärung der Mitarbeiter über Bedrohungen und die Gefahren für das eigene Unternehmen.“

WALTER JÄGER,
General Manager bei
Kaspersky Lab DACH



falsche Hände geraten, beispielsweise wenn Laptops oder Smartphones irgendwo vergessen oder verloren werden. Gegen Verlust oder Diebstahl hilft nur eine vollständige Verschlüsselung der Daten auf dem Gerät. Den Zugang zu den Daten erschweren bereits häufig wechselnde Passwörter: Dies

können auch, je nach System und Einsatzbereich, biometrische Verfahren wie etwa Fingerabdruckleser sein. Es ist jedenfalls wichtig, dass die Policy genau festlegt, wer im Fall von Verlust oder Diebstahl zu benachrichtigen ist. So kann derjenige das verloren gegangene Gerät unmittelbar vom Zugang zum Netz ausschließen. Bei Smartphones oder Handys wird die SIM-Karte sofort gesperrt.

Und schließlich bilden Malware und Softwarefehler ebenfalls ein erhebliches Risiko. „Gegen das Risiko durch Malware helfen nur eine aktuelle Schutzsoftware und die Aufklärung der Mitarbeiter über Bedrohungen und die Gefahren für das eigene Unternehmen“, erklärt Walter Jäger, General Manager bei Kaspersky Lab DACH. „Ebenso sollten alle installierten Programme und Betriebssysteme immer aktuell gehalten werden, um zusätzlich auch Softwarefehler zu vermeiden.“

Deutlich mehr Aufwand als der Schutz der Geräte verursacht die Absicherung der Zugangsnetze. Wenn Mitarbeiter von unterwegs zum Beispiel per WLAN über öffentliche Hotspots auf das Unternehmensnetz ➤



SICHERHEITSRICHTLINIEN: Die sogenannten Policies für Notebooks, WLAN-Netze, PDAs und Handys stellen fest, welche mobilen Geräte die Mitarbeiter für den Zugriff auf Unternehmensanwendungen benutzen dürfen.



„Idealerweise können sich drahtlose Geräte auch auf dem Firmengelände die Netzwerkressourcen nur über Access Points zugänglich machen, die in Verbindung mit der Firewall stehen, um Sicherheitsregeln abzubilden: Die Mitarbeiter gehen ihren Tätigkeiten nach, als wären sie auf Reisen.“

SVEN JANSSEN, Country Manager Germany bei SonicWALL

› zugreifen, garantiert ein virtuelles privates Netz (VPN) mit einem von der IT-Abteilung kontrollierten Endpunkt die bestmögliche Sicherheit, lautet die Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

In der Tat werden VPNs oft benutzt, wenn es darum geht, Mitarbeitern außerhalb eines Unternehmens Zugriff auf das interne Netz zu gewähren. Dabei baut der Computer des Mitarbeiters eine VPN-Verbindung zu dem ihm bekannten VPN-Gateway (Computer) der Firma auf. Über diesen „Tunnel“

ist es nun möglich, Informationen zu kommunizieren. Eine VPN-Software erlaubt es, die Daten zu verschlüsseln und sie an eine Gegenstelle zu senden.

Ein VPN ist allerdings nur dann sicher, wenn nicht gleichzeitig die Möglichkeit besteht, eine direkte Verbindung ins Internet zu erstellen. In diesem Fall wird das VPN zur Schwachstelle und dient als Einfallstor zum Firmennetz. Überhaupt können alle Geräte mit einer IP-fähigen drahtlosen Schnittstelle, ob Bluetooth, WLAN, GPRS oder UMTS, zu einer Bedrohung für das Firmennetz werden,

wenn sie wieder mit ihm verbunden sind. Einerseits können sie infiziert sein, andererseits kann es passieren, dass die Schnittstelle noch aktiv ist. Somit ist ein eventueller Angreifer in der Lage, das Gerät als Router oder Bridge zu nutzen und sich so in das Firmennetz einzubinden. „Dagegen hilft es, mithilfe von Skripten zu testen, ob sich das Gerät im Firmennetz befindet, und wenn dies der Fall ist, alle drahtlosen Schnittstellen abzudrehen“, rät Sven Janssen, Country Manager Germany bei SonicWALL. „Oder es wird veranlasst, dass sich drahtlose Geräte auch auf dem Firmengelände die Netzwerkressourcen nur über Access Points zugänglich machen können, die in Verbindung mit der Firewall stehen, um Sicherheitsregeln abzubilden: Die Mitarbeiter gehen ihren Tätigkeiten nach, als wären sie auf Reisen.“

ZENTRALE KONTROLLE

Abschließend nicht zu vergessen: mobile Mitarbeiter, die VoIP (Voice over IP: Internet-telephonie) nutzen. Dies erfolgt meistens über WLAN und öffentliche Hotspots. Um das Telefonieren über digitale Netze abhörsicher zu machen, gibt es ebenfalls die Möglichkeit, ein VPN einzusetzen. Bei einem VPN werden mittels IPsec eine Zugangskontrolle sowie die Datenintegrität, die Teilnehmerauthentisierung und die komplette Verschlüsselung der Sprachdaten sichergestellt. Für den Schutz von VoIP-Verkehr eignet sich dennoch der Standard SRTP (Secure-Real-Time Transport Protocol) am besten – es handelt sich um ein Protokoll, das die



Signalisierungsdaten und die Nutzdaten verschlüsselt, und dies ohne Qualitätsverlust der Sprachübertragung.

Was die heute zur Verfügung stehende Technologie angeht, sind also die Voraussetzungen dafür vorhanden, eine zwar nicht hundertprozentige, aber doch relativ gute Sicherheit beim Arbeiten fern des Firmengeländes zu garantieren. Doch ist eine Kette nur so stark wie ihr schwächstes Glied. Und wie sooft ist es der Mensch, der durch Achtlosigkeit die strengsten Maßnahmen zunichtemacht. Deshalb sind Unternehmen und ihre Administratoren gut beraten, das Management der externen Netzwerkzugänge zu zentralisieren, um diese besser kontrollieren zu können. Angenehme Nebenwirkung: eine beträchtliche Senkung der IT-Kosten.

NEUE ARBEITSMODELLE

Eins müssen Unternehmen wissen: In Zukunft kommen sie nicht darum herum, über ihre Ausrüstung in Sachen Mobile Computing nachzudenken. Und früher oder später, eher früher als später, werden sie sich auf den Wandel, der in der Arbeitswelt bereits begonnen hat, einstellen müssen. Denn die Trends, die sich bereits seit einigen Jahren abzeichnen, werden den Betrieben andere als die bisher praktizierten Arbeitsmodelle aufzwingen. So bewirkt die aufgrund des Abbaus von Handelshemmnissen, der Entstehung transnationaler Freihandelszonen und der Entwicklung globaler Finanzmärkte zügig fortschreitende Globalisierung, dass immer mehr Güter und Dienstleistungen – und damit zugleich Arbeitsplätze – im globalen Wettbewerb stehen.

Hinzu kommt die Tatsache, dass die Generation, die bereits auf den Arbeitsmarkt kommt, sich schon lange aller digitalen und mobilen Kommunikationsmöglichkeiten bedient und eine entsprechende IT-Ausstattung am Arbeitsplatz als selbstverständlich betrachtet. Inzwischen lautet die Frage nicht mehr, ob ein Unternehmen mobile Technologien nutzen, sondern welche es einsetzen soll.

Die größten Schwierigkeiten in Sachen „mobiles Arbeiten“ sollte also nicht die Technik bereiten, vorausgesetzt, Unternehmen



FAKTOR MENSCH: Wie so oft ist es der Mensch, der durch Achtlosigkeit die strengsten Maßnahmen zunichtemacht.

berücksichtigen die Sicherheitsaspekte genügend. Kritischer sieht es schon aus, was das angeht, was der Soziologe Richard Sennett, Autor des Buches „Der flexible Mensch“ (The Corrosion of Character), 1998 die „Risiken wachsender Flexibilisierung“ nennt. Seines Erachtens messen die Menschen infolge der Flexibilisierung der Arbeitswelt bestimmten Werten wie etwa Verantwortungsbewusstsein, Loyalität oder Arbeitsmoral deutlich weniger Bedeutung bei. Zudem fällt es ihnen immer schwerer, von der schnellen Erfüllung ihrer Wünsche abzusehen und nachhaltige Ziele zu verfolgen. Ein stets höher werdendes Arbeitstempo sowie kontinuierlich wachsende Leistungsanforderungen gepaart mit der ansteigenden Unsicherheit der Arbeitsverhältnisse und der Notwendigkeit, den Wohnort für den Beruf häufig wechseln zu müssen, bilden den Hintergrund des neuen Arbeitslebens.

In den Unternehmen werden unbeugsame Hierarchien durch selbstverantwortliche Teams ersetzt. Der Druck auf den Einzelnen steigt, begleitet von einer immer strenger werdenden Kontrolle der gesamten Produktionsabläufe und der Arbeitenden selber dank moderner Technik. Sennett will sogar noch eine weitere Konfliktquelle sehen, bestimmt durch den Gegensatz zwi-

schen den Werten, die Eltern ihren Kindern weitergeben möchten, und solchen, die ihr Berufsleben bestimmen.

Durch alle diese Begebenheiten könne sich eine Stimmung der Hilflosigkeit und der Instabilität, gar der Angst in weiten Teilen der Gesellschaft verbreiten, die eine Ellenbogengesellschaft begünstige.

STEIGENDE ANFORDERUNGEN

Unumstritten ist schon, dass die Mobilitätsanforderungen an den Einzelnen demnächst noch steigen werden. Deshalb sollten Unternehmen tunlichst daran arbeiten, die dafür notwendigen Rahmenbedingungen so menschlich wie möglich zu gestalten. Und vor allem sollten sie sich nicht davor scheuen, ihre Mitarbeiter an dieser Gestaltung aktiv teilnehmen zu lassen, anstatt nur zu verlangen, dass sie sich wortlos fügen. Mit Anordnungen alleine ist es längst nicht getan, und nur durch eine Firmenkultur, die eine gelungene Gratwanderung zwischen Selbstbestimmung und der nötigen Anpassung vollzieht, haben sowohl Unternehmen als auch ihre Beschäftigten eine Chance, sich in der Arbeitswelt von morgen einen festen Platz zu sichern.

Graziella Mimic ■