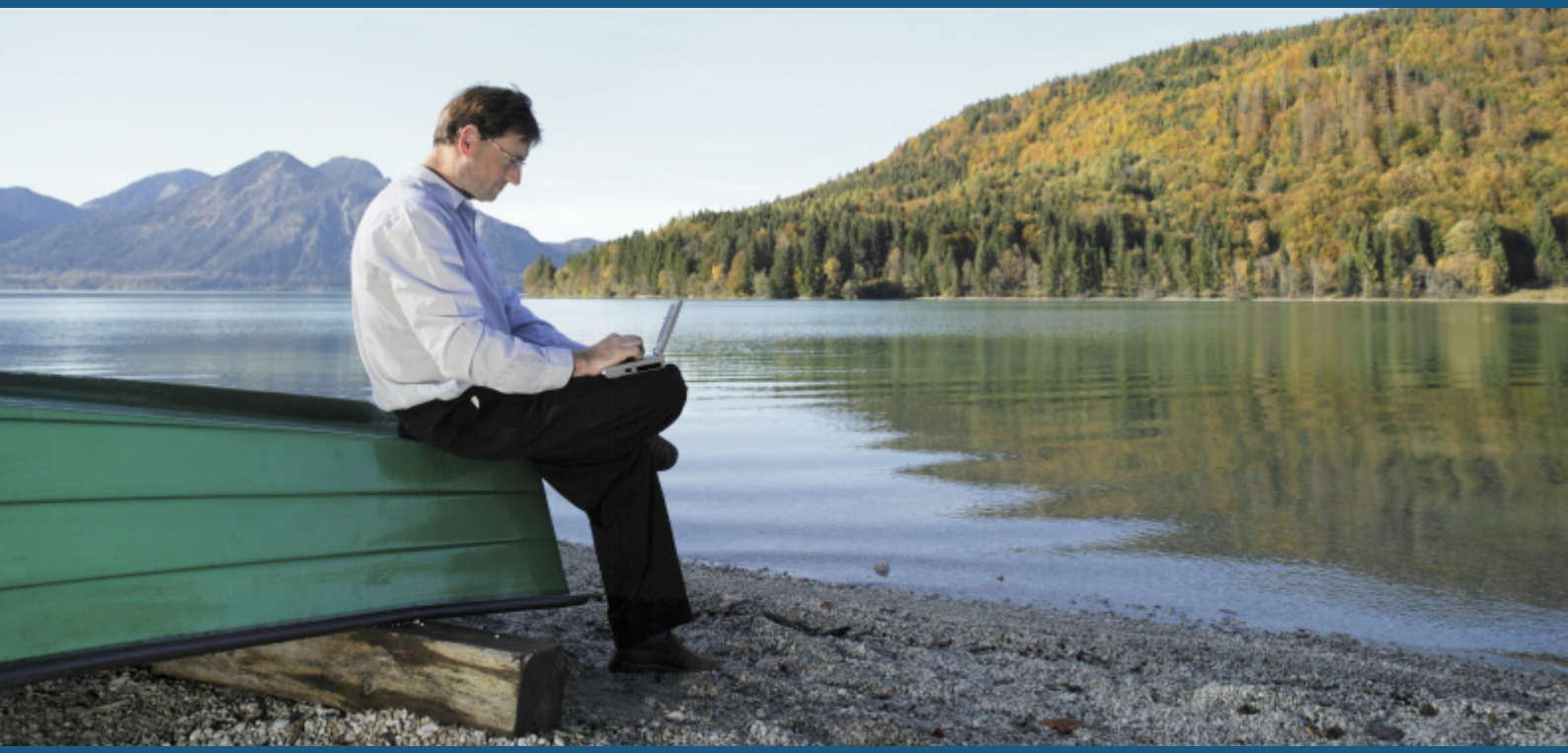
Whitepaper

Terminalserver-Technik und Virtualisierung als Plattform moderner BYOD-Konzepte



Leitfaden zur Einbindung privater Endgeräte in das Firmennetzwerk

H+H Software GmbH

Vorwort

Bisher kommt das Konzept BYOD, eine Abkürzung für „Bring Your Own Device“, vor allem bei Hochschulen und Universitäten zum Einsatz. BYOD bedeutet dabei nichts anderes, als dass die Studenten ihre eigenen Endgeräte – seien es Notebooks, Tablet-PCs oder Smartphones – mitbringen und Zugang zum Campus-Netzwerk erhalten.

Der Trend zum Einsatz von privaten Endgeräten hat mittlerweile auch Industrieunternehmen erreicht. In Deutschland und Europa ist man zwar noch bei den ersten zaghaften Annäherungen, aufhalten lassen wird sich das Konzept jedoch nicht mehr – zumal eine zunehmende Zahl an Arbeitnehmern nach BYOD-Lösungen verlangt. Der Grund dafür ist einfach: Fast jeder Arbeitnehmer besitzt heute mindestens ein privates IT-Endgerät, das er auch am Arbeitsplatz benutzen möchte. Sei es nur für die private E-Mail-Kommunikation oder aber als vollwertiges Arbeitsgerät.

Technisch stellt die Einbindung eines privaten Endgeräts in das Firmennetzwerk keine große Herausforderung dar. Möchte ein Unternehmen jedoch sicherstellen, dass mit sensiblen Daten im Sinne von Datenschutz und Datensicherheit umgegangen wird und lizenzrechtliche Aspekte bei der Nutzung von Anwendungen berücksichtigt werden, wird der Sachverhalt schon deutlich komplexer. Doch warum sollten sich Unternehmen das dann überhaupt antun? Die Antwort darauf geben die Mitarbeiter. Sie fühlen sich dem Unternehmen durch solche Maßnahmen verbundener, arbeiten effizienter, da sie flexibler in der Wahl des Arbeitsgerätes sind.

Wird das BYOD-Konzept konsequent umgesetzt, kann das auch die Gesamtbetriebskosten der EDV-Infrastruktur senken – zumindest dann, wenn die Mitarbeiter teilweise an den Kosten der ihnen zur Verfügung gestellten Geräte beteiligt werden. Oder sie nutzen vollständig privat finanzierte Endgeräte und erhalten einen finanziellen Ausgleich vom Arbeitgeber. Derartige Szenarien wiederum führen zu rechtlichen Fragen, die es im Vorfeld zu klären gilt, etwa im Falle eines Defekts oder Diebstahls des BYOD-Gerätes.

Management Summary / Abstract

Aktuellen Studien zufolge nutzen vor allem junge Arbeitnehmer schon heute ihre privaten Endgeräte in ihrem Arbeitsumfeld. Allein in Deutschland liegt der Anteil der 20- bis 29-jährigen bereits bei 78 Prozent. Bisher geht es allerdings vorwiegend darum, dass Arbeitnehmer am Arbeitsplatz private Anwendungen auch während der Arbeitszeit oder zumindest in den Pausen nutzen können. Das Gros machen dabei bisher soziale Netzwerke wie Facebook oder Twitter aus. Immerhin dulden laut einer Umfrage auf der CeBIT 2012, die vom Workplace-Management-Anbieter Matrix42 durchgeführt wurde, 62 Prozent der Arbeitgeber, dass ihre Mitarbeiter private Endgeräte für berufliche Zwecke nutzen. Im Umkehrschluss heißt das aber auch, dass ein nicht unerheblicher Teil dieser Arbeitnehmer private Endgeräte ohne das Wissen des Arbeitgebers nutzt – und viele davon sind sich der Risiken für die Unternehmens-IT durchaus bewusst. Andere Umfragen ergeben wiederum ein völlig anderes Bild: Vor allem in den USA wünschen Mitarbeiter sich BYOD-Konzepte, um auch in der Freizeit oder unterwegs einen Teil ihrer beruflichen Aufgaben erledigen zu können. Diese Veränderung der Arbeitsweise birgt Vorteile und Risiken gleichermaßen.

Das Konzept BYOD – Bring Your Own Device – legalisiert nun sozusagen die Nutzung privater Endgeräte innerhalb von Unternehmen. Dabei geht es nicht mehr nur um private Anwendungen, die auf den Geräten ausgeführt werden. Vielmehr avancieren die BYOD-Clients dann zu vollwertigen Arbeitsgeräten. Und davon profitieren nicht nur die Nutzer der BYOD-Geräte. Unternehmen können ihre Mitarbeiter auf diese Weise motivieren und stärker an sich binden. Sie erhalten das Image einer modernen, fortschrittlichen Organisation, das bei der Suche nach neuen, hochqualifizierten Mitarbeitern den Ausschlag geben kann. Hinzu kommt auch eine Kostenreduktion, da private Endgeräte nur teilweise oder gar nicht vom Arbeitgeber finanziert werden müssen. Für Arbeitnehmer liegen die Vorteile im Wesentlichen darin, dass sie Geräte nutzen können, die optisch und technisch ihren Vorstellungen entsprechen und nicht ständig zwischen beruflichen und privaten Geräten hin- und herwechseln müssen.

Bei der Umsetzung eines BYOD-Konzeptes resultieren jedoch sowohl für die Organisation als auch für ihre Mitglieder gewisse Herausforderungen. Die Nutzung privater Endgeräte kann die Komplexität der IT-Infrastruktur und den erforderlichen Administrationsaufwand erhöhen. Zusätzliche sicherheitsrelevante sowie lizenzrechtliche Aspekte sind zu bedenken und auch das Thema Rechtssicherheit darf nicht außer Acht gelassen werden.

Ein möglicher Weg ist die Terminalserver-Technik, die bereits in vielen Unternehmen zur Vereinfachung der Administration komplexer Infrastrukturen zum Einsatz kommt. Auch die Desktop-Virtualisierung kann als Basis für die Einbindung privater Endgeräte ins Unternehmensnetzwerk dienen. Beide Technologien bringen bereits gute Voraussetzungen für BYOD mit. Idealerweise werden sie jedoch um zusätzliche Lösungen zur Steuerung von Anwendungen, lokalen Laufwerken und Zugriffsrechten ergänzt. Auch BYOD-Speziallösungen gibt es mittlerweile von einigen namhaften Anbietern. Entsprechende Produkte führen z. B. eine logische Trennung privater und beruflicher Programme und Daten auf dem Endgerät durch.

NetMan Desktop Manager 5 von H+H ist eine Erweiterung der Microsoft Remote Desktop Services, die insbesondere das Veröffentlichen von Anwendungen vereinfacht und zu einem gewissen Grad automatisiert. Die verwendete Terminalserver-Technologie stellt einen effizienten Weg zur Umsetzung des BYOD-Gedanken in Unternehmen dar, ohne lizenzrechtliche und sicherheitsrelevante Aspekte zu vernachlässigen.

BYOD – eine kurze Begriffserklärung

Der noch junge Begriff BYOD steht für die Umschreibung eines modernen IT-Konzepts: Bring Your Own Device, was nichts anderes bedeutet, als dass Mitglieder einer Organisation ein privates Endgerät auf dem Gelände und im Netzwerk der Organisation nutzen. BYOD umfasst dabei auch den Zugriff auf das Netzwerk, Server und Anwendungen der Organisation mithilfe organisationsfremder Endgeräte. Dabei handelt es sich typischerweise um mobile Endgeräte wie Smartphones, Tablet PCs und Notebooks. Vom Konzept des BYOD versprechen sich die Organisationen ebenso wie ihre Mitglieder Vorteile unterschiedlicher Natur. Auf Seiten der Organisation stehen eine mögliche Kostenersparnis, längere Nutzungsdauer der Endgeräte sowie eine bessere Mitgliederbindung. Die Mitglieder selbst erhalten eine größere Flexibilität in der Auswahl des Endgerätes, was zu einer höheren Motivation und Zufriedenheit führen soll. Eine Reihe von Nachteilen bringt BYOD auch mit sich. Zum einen nehmen Komplexität des Organisationsnetzwerkes und dessen Administrationsaufwand zu. Zum anderen sind rechtliche Aspekte im Umgang mit dem BYOD-Endgerät zu bedenken.

Die Endgeräte: Smartphone und Tablet vs. Notebook

Bei der Umsetzung eines modernen BYOD-Konzeptes spielen die eingesetzten Endgeräte eine große Rolle. Ein Großteil der Arbeitnehmer in Industrieunternehmen besitzt mittlerweile ein privates Smartphone oder einen Tablet PC. Als Betriebssysteme kommen dabei vorwiegend Google Android, Apple iOS und – erheblich seltener – die Mobilvarianten von Microsoft Windows zum Einsatz. All diesen Plattformen gemein ist die Eigenschaft, keine Standard-PC-Programme ausführen zu können. Vielmehr arbeiten diese Geräte mit so genannten Apps, kleinen Anwendungen, die speziell für die jeweilige Plattform entwickelt wurden. Als Arbeitsgeräte im Produktivbetrieb sind Smartphones und Tablets gleichermaßen ungeeignet. Dazu reicht einerseits oft einfach die Rechenleistung nicht aus, andererseits disqualifizieren fehlende Schnittstellen und die meist nur virtuell vorhandenen Tastaturen diese Geräte für den ernsthaften Arbeitseinsatz. Dennoch wünschen sich viele Arbeitnehmer einen Zugriff auf das Unternehmensnetzwerk und bestimmte Daten. Dabei handelt es sich in erster Linie um Synchronisationsvorgänge für Kalendereinträge, Kontakte und Notizen, die eben auch auf dem Smartphone oder dem Tablet verfügbar sein sollen. Für den Administrator stellt dieses Szenario keine echte Herausforderung dar. Die entsprechenden Rechte und Restriktionen lassen sich noch recht einfach mit den Bordmitteln des im Organisationsnetzwerk genutzten Server-Betriebssystems durchsetzen.

Bedeutend anspruchsvoller wird es, wenn es um vollwertige Notebooks geht. Diese Geräte sind ab einer Displaygröße von etwa 13 Zoll auch für produktives Arbeiten geeignet. An Rechenleistung, Speicherkapazität und Schnittstellenvielfalt stehen moderne Notebooks Desktop PCs kaum mehr nach. Und auch die aktuell meist verwendeten Chiclet-Tastaturen ermöglichen schnelles und ermüdungsfreies Tippen. Hinzu kommt, dass ein Notebook alle Daten und Anwendungen verarbeiten kann, die innerhalb einer Organisation genutzt werden. Für eine ernsthafte Umsetzung des BYOD-Konzeptes kommen letztlich nur vollwertige Notebooks infrage. Denn während Smartphones und Tablets eher dem professionellen Konsum digitaler Inhalte (Analysen, Auswertungen, Statistiken etc.) dienen, eignen sich Notebooks dank der größerer Bildschirme, vollwertiger Tastaturen und entsprechender Anwendungen für den vollwertigen Produktiveinsatz – sowohl privat als auch am Arbeitsplatz. Hier müssen die Mitarbeiter vollen Zugriff auf alle Daten und Anwendungen erhalten, die sie im Arbeitsalltag benötigen. Auch das Verändern bestehender und das Erstellen neuer Daten muss gewährleistet sein. Damit gehen aber auch große Sicherheitsrisiken für die IT-Infrastruktur und den Datenbestand der Organisation einher. Die Gefahren gehen dabei sowohl von der Person aus, die das BYOD-Gerät nutzt, als auch von privat genutzten Anwendungen und Daten.

Wenn Unternehmen ihren Mitarbeitern die Benutzung privater Endgeräte im Unternehmensnetzwerk ermöglichen, sollten präzise Mindestanforderungen in Bezug auf die Hardwareausstattung festgelegt werden. Auch bestimmte Sicherheitsprogramme wie Virenscanner und -wächter sowie Tools zum Aufspüren von Spy- und Malware sollten bei einem BYOD-Gerät zwingend vorhanden sein und regelmäßig geprüft werden.

Sonderfall: Der Bildungssektor

Im Gegensatz zu Industrieunternehmen die gewinnorientiert arbeiten, finanzieren sich Schulen, Hochschulen und Universitäten weitestgehend aus öffentlichen Mitteln. Das führt gerade bei Schulen oftmals zu finanziellen Engpässen, wenn es um die Bereitstellung einer leistungsfähigen IT-Infrastruktur geht. Denn der Computer ist als Lehr- und Lernmittel aus einem modernen Unterricht nicht mehr wegzudenken. Hier kann das BYOD-Konzept nachhaltig Abhilfe schaffen. Hochschulen und Universitäten setzen heute schon auf BYOD und sind bereits Vorbild für manche Schulen. Hier nutzen Schüler private, von den Eltern finanzierte Notebooks im Unterricht. Die Schulträger müssen diese hohen Investitionen nicht mehr tätigen und können das knappe Haushaltsbudget in eine technisch und pädagogisch moderne Infrastruktur investieren. Mithilfe entsprechender pädagogischer Oberflächen wie etwa NetMan for Schools gelingt auch die sichere und zuverlässige Einbindung der privaten Notebooks in das Schulnetzwerk und damit in den Unterricht.

BYOD – Herausforderung für Unternehmen und Mitarbeiter

Auf den ersten Blick scheint BYOD nur für die Organisation, die ihren Mitgliedern die Nutzung privater Endgeräte ermöglicht, mit technischen Herausforderungen verbunden zu sein. Doch auch die Nutzer der BYOD-Clients müssen den Einsatz ihres privaten Gerätes kritisch hinterfragen. Auf Unternehmensseite geht es in erster Linie um den Schutz geschäftskritischer und personenbezogener Daten sowie um die Aufrechterhaltung eines reibungslosen Betriebs der IT-Infrastruktur. Auf Arbeitnehmerseite sehen die Herausforderungen ganz anders, aber deswegen nicht geringer aus. So wollen auch sie ihre privaten Daten und Anwendungen vor fremdem Zugriff geschützt wissen. Und sie laufen Gefahr, keine klare Abgrenzung zwischen Beruf und Freizeit zu finden. So kann ein innovatives Konzept wie BYOD auch leicht in einer Überbeanspruchung der Mitarbeiter-Ressourcen enden, wenn Mitarbeiter über die Regelarbeitszeit hinaus dem Unternehmen zur Verfügung stehen (müssen).

Auch der juristischen Betrachtung müssen sich BYOD-Projekte stellen. Gerade im Falle eines Verlustes des privaten oder zur privaten Nutzung zu Verfügung gestellten Endgerätes muss klar geregelt sein, wer zu welchem Anteil für den Schaden aufkommt. Dasselbe gilt bei Defekten des BYOD-Gerätes. Hier gilt es vorab zu klären, welche Art von Beschädigungen an Hard- oder Software vom Unternehmen, welche vom Nutzer getragen werden müssen. Spezielle Endgeräteversicherungen können Streitigkeiten vorbeugen, verursachen aber zusätzliche Kosten.

Hinzu kommen lizenzrechtliche Aspekte und die Frage nach dem Support für privat genutzte Endgeräte. Wie handhabt das Unternehmen Fälle, in denen das Endgerät aufgrund der privaten Nutzung in seiner Benutzbarkeit beeinträchtigt wird? Dabei muss es keinen physikalischen Schaden davontragen. Auch die Installation schadhafter Software oder tiefgreifende Veränderungen am Betriebssystem kommen als Ursache infrage. Steht die IT-Abteilung bei Fragen auch außerhalb der normalen Arbeitszeiten zur Verfügung oder muss sich der BYOD-Nutzer an Dritte wenden? Abhilfe könnte hier eine so genannte „Self-Support-Zone“ schaffen. Dabei warten Mitarbeiter mit hohem technischem Verständnis und geringer Sicherheitsstufe das eigene Endgerät und die von Kollegen in Eigenregie. Der Arbeitgeber stellt ihnen dafür ein bestimmtes Zeitkontingent zur Verfügung.

Eine aktuelle Umfrage von TNS Infratest kommt zu dem Ergebnis, dass sich nahezu alle Organisationen der Risiken beim Einsatz privater Endgeräte bewusst sind. Doch noch nicht einmal die Hälfte dieser Organisationen hat bereits verbindliche Regelungen für den Umgang mit BYOD-Endgeräten festgelegt, geschweige denn die Risiken und Gefahren mithilfe entsprechender Lösungen ausgemerzt.

Die Kostenseite

Organisationen, die bereits BYOD-Konzepte nutzen oder über deren Einführung nachdenken, geben als Gründe meist höhere Flexibilität und gesteigerte Produktivität ihrer Mitglieder an. Das ergibt eine Umfrage unter 328 deutschen Unternehmen im Auftrag von Dell. Dass BYOD auch zu einer nachhaltigen Kostensenkung führen kann, scheint für viele Organisationen hingegen nur von zweitrangiger Bedeutung zu sein. Dabei ist das Sparpotenzial durchaus beachtlich. Wird das BYOD-Konzept konsequent in die Tat umgesetzt, finanziert nicht länger die Organisation selbst die IT-Endgeräte. Vielmehr geht dieser Kostenblock zu Lasten der Mitglieder – zumindest teilweise. Denn selbst wenn die Organisationen ihren Mitgliedern einen Ausgleich für die Nutzung privater Endgeräten bezahlt und das Einbinden der BYOD-Geräte den Administrationsaufwand erhöht, ist eine messbare Kostenersparnis möglich. Dem entgegen steht allerdings die Vermutung, dass Geräte, die privat und beruflich genutzt werden, einem höheren Verschleiß unterliegen und aufgrund der kürzeren Lebensdauer wieder einen Kostenmehraufwand bedeuten. Für eine genauere Betrachtung dieses Aspekts fehlt es bisher jedoch an entsprechenden Langzeiterfahrungen.

Terminalserver und Virtualisierung vereinfachen BYOD

Unternehmen, die ein so modernes und gleichzeitig komplexes IT-Konzept wie BYOD in die Tat umsetzen wollen, sollten über eine ebenso moderne Infrastruktur verfügen. In klassischen Client-Server-Netzwerken, die grundsätzlich schon einen recht hohen Administrationsaufwand erfordern, würde BYOD die Komplexität noch einmal stark erhöhen. Ideale Voraussetzungen hingegen bieten zentral administrierbare EDV-Infrastrukturen wie etwa Terminalserver-Netzwerke oder virtualisierte Umgebungen. In beiden Fällen bleiben unternehmenseigene Daten und Anwendungen physikalisch stets innerhalb des Unternehmensnetzwerkes. Die beruflich und privat genutzten Endgeräte dienen lediglich als Anzeige-Terminals für Bildschirminhalte.

Die Remote Desktop Services von Windows bieten schon eine ganze Reihe an Funktionen zur Veröffentlichung von Anwendungen. Dennoch reichen die Sicherheitsmechanismen und der Komfort der Gruppenrichtlinien nur für „einfache“ BYOD-Endgeräte wie Smartphones oder Tablet PCs aus. Für komplexe Clients wie Notebooks oder Desktop PCs mit vollwertigem Betriebssystem sollten Organisationen über die Anschaffung einer Erweiterung der Remote Desktop Services wie H+H NetMan Desktop Manager 5 nachdenken. Damit stehen dem Administrator zusätzliche Funktionen unter einer komfortablen Oberfläche zur Verfügung, die das Veröffentlichen von Anwendungen, die Vergabe von Rechten und die Kontrolle über lokale Laufwerke erheblich vereinfachen.

Bei der Einbindung der BYOD-Geräte in einem Terminalserver-Netzwerk führen verschiedene Wege zum Ziel. Wird den Nutzern etwa der Zugang zu benötigen Anwendungen und Daten über ein Web-Interface zur Verfügung gestellt, ist nicht einmal die Installation irgendwelcher Software-Programme auf dem BYOD-Gerät erforderlich. Hinzu kommt, dass ein Web-Interface plattformunabhängig agiert und somit die Einbindung jeglicher Endgeräte ermöglicht – egal, ob Smartphone, Tablet PC, Notebook oder Desktop PC, ob Windows, Mac OS oder Linux. Mehr Komfort bietet allerdings die Installation eines lokalen Clients. Hiermit lassen sich benötigte Anwendungen dynamisch in den Desktop des BYOD-Endgeräts integrieren, sie sind wie gewohnt bequem aus dem Startmenü heraus und über Desktop-Verknüpfungen ausführbar. Selbst ein Doppelklick auf eine Datei öffnet automatisch die korrespondierende Anwendung – ganz wie bei einem lokalen System. Für den Mitarbeiter ist so auch eine klare Trennung zwischen Beruf und Freizeit erreichbar – technisch wie zeitlich. Denn erst wenn der Mitarbeiter seinen Arbeitstag beginnt, startet er den Client und erhält damit Zugriff auf berufliche Anwendungen und Daten. Nach seiner Arbeit, etwa zum Feierabend, beendet er den Client wieder. Dann befinden sich auf dem BYOD-Endgerät ausschließlich seine privaten Programme und Dateien – sofern er das wünscht. In diesem Fall hat er weder Zugriff auf Unternehmensdaten noch kann er seine beruflichen E-Mails abrufen oder Termine planen. Ist das Endgerät über den Client mit dem Unternehmensnetzwerk verbunden, besteht dennoch kein Risiko des Datenverlustes oder der -Manipulation, da alle Programme und Daten ausschließlich auf zentralen Server gesichert sind und auch nur dort ausgeführt werden. Damit wird der Datensicherheit ebenso wie dem Datenschutz Rechnung getragen.

Dank effektiver Beschleunigung des RDP-Protokolls ermöglicht NetMan Desktop Manager 5 auch mobilen Mitarbeitern und Heimarbeitskräften die bestmögliche User Experience beim Arbeiten mit zentral bereitgestellten Anwendungen und Daten. Dazu trägt auch der Umstand bei, dass der BYOD-Nutzer seine privaten Programme und Daten wie gewohnt nutzen kann. Lediglich der Zugriff auf das Unternehmensnetzwerk muss für diese Anwendungen reglementiert werden. Eine Trennung zwischen privaten und beruflichen Daten erfolgt bereits durch NetMan Desktop Manager 5.

Die VDI-Technologie (Virtual Desktop Infrastructure) bringt, wie die Terminalserver-Technik, beste Voraussetzungen für die konsequente Umsetzung des BYOD-Ansatzes mit. Im Gegensatz zu den Remote Desktop Services werden jedoch nicht nur Anwendungen und Daten auf dem Endgerät bereitgestellt. Kernpunkt von VDI ist die Übertragung vollständiger, virtueller Desktops an die Clients. Dazu zählen alle erforderlichen Anwendungen sowie das gesamte Windows-Betriebssystem inklusive aller persönlichen Einstellungen. Die Mitarbeiter arbeiten dann stets in dieser virtuellen Umgebung, was etwaige Sicherheitsrisiken weitgehend ausräumt. Für die Nutzung seiner privaten Anwendungen hat der User bei VDI zwei Möglichkeiten: Entweder er schaltet zeitweise vom virtuellen auf den lokalen Desktop um oder der Arbeitgeber erlaubt die Installation privater Software auf dem virtuellen Desktop. Diese Vorgehensweise ist zwar die komfortablere, birgt aber zusätzliches Gefahrenpotenzial. Diese geht einerseits von der privaten Software aus. Wobei der Arbeitgeber prüfen sollte, welche Programme der Arbeitnehmer installieren möchte. Andererseits müssen auch lizenzrechtliche Aspekte geklärt werden. Denn für eine zusätzliche Installation eines Programms benötigt der BYOD-Nutzer oftmals auch eine weitere Lizenz.

Aufgrund der recht hohen Komplexität von VDI-Umgebungen und der erforderlichen leistungsfähigen Hardware ist der Kostenaufwand pro Endgerät bei VDI jedoch deutlich höher als in einer vergleichbaren Terminalserver-Infrastruktur. Für jedes Endgerät, das Zugriff auf eine VDI-Umgebung erhalten soll, muss eine Virtual-Desktop-Access-Lizenz (VDA) angeschafft werden oder eine gültige Microsoft Software Assurance (SA) bestehen, die zusätzliche Kosten verursacht. Hinzu kommt, dass das Microsoft VDA-Lizenzierungsmodell das BYOD-Konzept bis dato nicht eindeutig abbildet. So ist eine VDA-Lizenz bzw. eine bestehende Software-Assurance zwar auf bis zu vier private Geräte (z.B. Tablets) übertragbar, dies gilt jedoch nur solange, wie diese privaten Geräte außerhalb der Firma eingesetzt werden. Sobald der Arbeitnehmer, diese Gerät als VDI-Client im Büro nutzen möchte, muss eine zusätzliche VDA-Lizenz beschafft werden. Nutzt er stattdessen das Tablet ausschließlich zuhause oder unterwegs, darf er ohne weitere Lizenzierung auf virtuelle Desktops zugreifen.

BYOD-Speziallösungen

Immer mehr Software-Firmen bieten mittlerweile spezielle BYOD-Lösungen oder Programme für das Mobile Device Management an. Diese sind jedoch überwiegend auf Tablets und Smartphones ausgelegt. Hierbei erfolgt eine Trennung zwischen beruflichen und privaten Anwendungen und Daten, etwa über eine Verschlüsselung auf dem Endgerät, die von zentraler Stelle aus vorgenommen wird. Die Nachteile einer BYOD-Speziallösung sind zusätzliche Kosten und eine weitere Software, die administriert werden muss. Modernere Lösungen erlauben mittlerweile ein umfassendes Handling von BYOD-Geräten, einschließlich vollwertiger PCs und Notebooks. Zu den wichtigsten Funktionen zählen das automatisierte Einbinden der Geräte in die Management-Oberfläche, die Anwendungs- und Datenbereitstellung sowie das Anpassen der Sicherheitseinstellungen anhand des Benutzers und des Endgerätetyps.