CORTADO

Business Class of Cloud Desktop Services

White Paper:

Integration von Smartphones und Tablets in die Unternehmens-IT

Integration von Smartphones und Tablets in die Unternehmens-IT

1 Einführung

Smartphones und Tablet-PCs sind auf dem Vormarsch und laufen PC und Notebooks den Rang ab. CIOs stehen heute nicht vor der Entscheidung, ob in ihrem Unternehmen Mobilgeräte eingesetzt werden sollen – diese Entscheidung ist längst gefallen oder wurde ihnen von ihren Mitarbeiter abgenommen, die ihre privaten Geräte oft auch für dienstliche Belange nutzen. Einer Umfrage von PAC bei 169 CIOs deutscher Unternehmen mit mehr als 50 Mitarbeitern im April 2011 zufolge gehört der mobile Zugriff auf E-Mail, Kalendersysteme und Kontaktverzeichnisse mittlerweile in rund 80 Prozent der befragten Unternehmen zum Standard.

Trotzdem steckt die systematische Nutzung mobiler Geräte für den Zugriff auf Unternehmensdaten und -anwendungen noch in den Kinderschuhen. So nutzten nur ca. 20 Prozent der befragten Unternehmen mobile Lösungen zur Optimierung von Geschäftsprozessen wie zum Beispiel mobile ERP- oder CRM-Applikationen. Gründe dafür sind nicht zuletzt ein unübersichtlicher Mobilgerätemarkt, fehlendes Know-how zur Umsetzung mobiler Prozesse, Unsicherheiten in Bezug auf die Auswahl der passenden Technologie sowie berechtigte Sicherheitsbedenken. Das vorliegende Whitepaper adressiert genau diese Punkte, um Unternehmen dabei zu unterstützen, die Potenziale des mobilen Computings optimal und sicher zu nutzen.

2 Chancen und Herausforderungen von Enterprise Mobility

2.1 Smartphones und Tablets: Bestandsaufnahme

Die Zahl der weltweit verkauften Smartphones wird sich laut Gartner von einer geschätzten halben Milliarde in 2011 voraussichtlich bis 2015 auf 1,1 Milliarden verdoppelt haben. Schon jetzt gibt es eine kaum überschaubare Fülle von Gerätetypen von zahlreichen Herstellern, und auch bei den Betriebssystemen für Mobilgeräte ist Bewegung im Markt. Der langjährige Marktführer Symbian hat nach dem Umstieg von Nokia auf Windows Phone in 2011 mehr als 50 Prozent Marktanteile eingebüßt. Für den Palm-OS-Nachfolger WebOS von HP werden seit 2011 keine mobilen Geräte mehr entwickelt.

Laut Gartner sind die in nächster Zukunft relevantesten Betriebssysteme für Smartphones Android von Google, iOS von Apple, BlackBerry OS von Research in Motion (RIM) und Windows Phone von Microsoft. Dabei sieht Gartner bis 2015 Android als den unangefochtenen Marktführer mit knapp 50 Prozent Marktanteil, zunächst gefolgt von iOS und BlackBerry OS, die geringfügig Marktanteile abgeben, und einem – Nokias Erfolg vorausgesetzt – sich bis 2015 auf 19 Prozent (Platz 2) steigernden Microsoft Windows Phone.

Bei den Tablets dagegen wird Apples iOS wohl seine souveräne Marktführerschaft (mit über 70 Prozent Marktanteil in 2011) bis 2015 behaupten können, gefolgt von Android und Microsoft Windows. Auch RIM, das in 2010 das Embedded-Betriebssystem QNX zugekauft hat, spricht Gartner mit dieser Plattform Chancen im Tablet-Markt zu. Mittelfristig sollen BlackBerry OS und QNX zu dem neuen Betriebssystem „BlackBerry 10“ verschmolzen werden.

Mobile Betriebssysteme mit Zukunft dürften in erster Linie Android und iOS sein, die zudem sowohl im Smartphone- als auch im Tablet-Segment die erfolgreichsten sind.

Bewertung und Einordnung

Android ist ein offenes System, dass auf zahlreichen Geräten von verschiedenen Herstellern und in unterschiedlichen Preisregionen läuft. Aufgrund der Offenheit der Plattform ist allerdings die Abstimmung von Betriebssystem und Hardware nicht immer optimal, so dass gute Android-Kenntnisse bei der Administration von Vorteil sind.

IOS ist dagegen ein geschlossenes System. Bei iPhones und iPads stimmt der Hersteller Hardware und Betriebssystem selbst aufeinander ab. Auch bei den Applikationen („Apps“) behält sich Apple ein hohes Maß an Kontrolle vor. Die Individualisierungsmöglichkeiten sind daher geringer. Auf der Habenseite steht eine sehr hohe Nutzerakzeptanz und die verlässliche Einhaltung der von Apple vorgegebenen Qualitätsstandards.

BlackBerry OS (ebenfalls geschlossen) ist noch immer die führende Plattform für Smartphones im Unternehmenseinsatz, nicht zuletzt wegen seiner flexiblen Administrierbarkeit und Sicherheit. Abzuwarten bleibt die weitere Entwicklung im Zusammenhang mit BlackBerry 10.

Ähnliches gilt derzeit auch für **Microsoft Windows Mobile / Window Phone**: Ein nachhaltiger Erfolg ist noch ungewiss (und hängt derzeit noch zu großen Teilen von Nokia ab). Abwarten heißt es auch bei einigen bisher nicht genannten Plattformen mit interessanten Ansätzen, darunter Bada von Samsung und das linuxbasierte Tizen (früher MeeGo).

Letztlich sollten allerdings in strategischer Hinsicht einzelne Plattformen keine entscheidende Rolle spielen (wenn nicht – etwa aus Sicherheitsgründen – ein streng homogener Bestand firmeneigener Mobilgeräte benötigt wird). Denn niemand kann heute mit Sicherheit sagen, was die Zukunft bringt. Deshalb fahren Unternehmen im Regelfall besser, wenn sie dafür sorgen, dass ihre mobile Infrastruktur verschiedene Geräte und Plattformen unterstützt und sicher integrieren kann (vgl. auch Kap. 3.2.).

2.2 Die Nutzenpotenziale mobiler Geräte im Unternehmenseinsatz

Der Nutzen eines effizienten Einsatzes mobiler Geräte im Unternehmen lässt sich folgendermaßen zusammenfassen:

- Mehr Leistungsfähigkeit und Produktivität
- Mehr Sicherheit
- Weniger Kosten

Verbesserte Leistungsfähigkeit

Wenn mobile Anwender viele ihrer Aufgaben auch von unterwegs direkt auf dem Smartphone oder Tablet-PC bearbeiten können, führt das zu beschleunigten und flexibleren Prozessen und verbesserter Unternehmensleistung: schnellere Entscheidungen, mehr Abschlüsse, kürzere Rechnungsprozesse und weniger Backoffice-Tätigkeiten.

Dabei ist das Ausmaß realisierbarer Nutzenpotenziale stark abhängig von den konkret auf dem Mobilgerät verfügbaren Funktionen und Daten. Projekte mit Enterprise-Applikationen wie CRM, ERP und Supply Chain Management sind jedoch sehr umfangreich und erfordern sorgfältige Planung meist mit Unterstützung

externer Berater. Einfacher, aber ebenfalls effektiv sind Maßnahmen, die dafür sorgen, dass Mitarbeiter so viele ihrer alltäglichen Office-Aufgaben wie möglich auch mobil mit ihrem Smartphone oder Tablet-PC erledigen können.

Dies erfordert insbesondere einen sicheren Zugriff auf Dateien im Unternehmensnetzwerk sowie auf wichtige Office-Funktionen wie Datenbankberichte, PDF-Erzeugung, Bearbeitungsfunktionen, Faxen oder Drucken. Optimal ist es, wenn das bestehende, unternehmenseigene Rechtesystem integriert wird – mit der Möglichkeit, die Rechte der Nutzer für mobile Geräte einzuschränken.

Verbesserte Reaktionsfähigkeit

Ein wichtiger Nutzenaspekt mobilen Arbeitens ist die Geschwindigkeit!

Viele, wenn nicht der größte Teil der anfallenden Aufgaben im Unternehmen, zum Beispiel die Beantwortung von Anfragen, Auftragsbestätigungen oder die gemeinsame Arbeit an Projekten, erfordern Zugang zu Informationen und Ressourcen im Unternehmensnetzwerk. Wenn Mitarbeiter über ihr Mobilgerät auf diese Informationen zugreifen können, sind sie in der Lage, wesentlich schneller auf neue Aufgabenstellungen zu reagieren.

Nach einer Studie von IpsosReid (2007) empfangen beispielsweise BlackBerry-Nutzer über 2500 zeitkritische E-Mails im Jahr. Wenn lediglich 10 Prozent dieser E-Mails nur mit Zugriff auf das Unternehmensnetzwerk und weitere 10 Prozent dadurch zumindest qualitativ besser beantwortet werden können, ergibt sich daraus bereits eine Verbesserung der Reaktionsfähigkeit des Unternehmens bei 500 Mails pro Mitarbeiter – und damit zufriedenere Kunden, mehr Abschlüsse oder auch rechtzeitige Schadensbegrenzungen.

Mehr Produktivität

Ein weiterer Vorteil besteht in der effizienteren Nutzung von Warte- und Reisezeiten.

Mitarbeiter mit mobilem Zugriff auf aktuelle Informationen sind fast genauso produktiv, als wenn sie gerade im Büro arbeiten würden. Nimmt man an, dass sich dadurch monatlich nur zwei Stunden zusätzlicher produktiver Zeit pro Mitarbeiter ergeben, entspräche das bei durchschnittlichen Gehaltskosten pro Mitarbeiter/Jahr von 60.000 Euro einer jährlichen Kostenersparnis von ca. 800 Euro je Mitarbeiter.

Bessere Zusammenarbeit

Der Zuwachs an Flexibilität durch mobile Prozesse führt zudem zu einer optimierten Zusammenarbeit, etwa bei der gemeinsamen Arbeit an Projekten. So muss die Teamarbeit nicht ruhen, bis wieder alle im Büro sind. Ob in der Flughafenlounge, im Zug, bei Kundenterminen oder beim Geschäftspartner: Jeder Mitarbeiter kann von seinem Standort aus auf dieselben Informationen zugreifen und auch selbst Dokumente im Projektordner ablegen. So haben alle Beteiligten Zugang zu den

aktuellsten Dateiversionen und können schneller auf veränderte Bedingungen reagieren. Das ist auch bei einzuhaltenden Freigabe-Workflows von Bedeutung: Auch wenn der Abteilungsleiter auf Dienstreise ist, kann er den Bericht abzeichnen und an die Chefetage weiterleiten.

Mehr Sicherheit

Mehr Sicherheit? Bringt nicht die Nutzung mobiler Geräte eher zusätzliche Sicherheitsprobleme mit sich? Das ist richtig – und genau diese Sicherheitsprobleme sind in den meisten Unternehmen längst Realität, nämlich überall da, wo Mitarbeiter ihre mobilen Geräte ohne sichere Einbindung in eine verlässliche Backend-Infrastruktur nutzen und zum Beispiel Unternehmensdaten bei unsicheren (womöglich privaten) Cloud-Diensten speichern, um sie mobil nutzen zu können.

Der Einsatz mobiler Geräte in Unternehmen setzt eine stringente Sicherheitsstrategie vorraus.

Deshalb sorgt der planmäßige, durchdachte Einsatz mobiler Geräte mit einer tragfähigen technologischen Basis und einer stringenten Mobilstrategie für mehr Sicherheit von Daten und Systemen. Bestandteile eines elementaren mobilen Sicherheitskonzepts sind die gesicherte Datenübertragung, eine zentrale Datenhaltung und die Integration in vorhandene Berechtigungskonzepte (siehe unten Kapitel 4).

Einsparpotenziale

Zusätzlich zu den Kosteneinsparungen durch eine höhere Produktivität ergeben sich weitere Einsparpotenziale durch die wesentlich kostengünstigere Infrastruktur mobiler Geräte. In Anschaffung und Wartung verursachen Mobilgeräte geringere Kosten als etwa Notebooks und sind auch schneller und günstiger ersetzbar. Mit der geeigneten technologischen Plattform kann zudem die vorhandene IT-Infrastruktur ohne zusätzliche Investitionen für die Integration und einfache Administration sämtlicher mobiler Geräte genutzt werden.

2.3 Die Herausforderungen beim Einsatz mobiler Geräte in Unternehmen

Einstiegsbarrieren

Unternehmen, die das Nutzenpotenzial mobilen Arbeitens ausschöpfen möchten, sehen sich einer Reihe von Herausforderungen gegenüber. Zunächst stellt sich die Frage, wie mobile Geräte möglichst effektiv – aber bei vertretbarem Aufwand – konkrete Unternehmensprozesse unterstützen können. Wenn etwa IDC fordert, vor der Implementierung mobiler Lösungen zunächst die Geschäftsprozesse gründlich zu analysieren, erzeugt das für viele Unternehmen eine Barriere, die sie hindert, die Mobilisierung überhaupt zu beginnen. Unternehmen können die Einstiegsbar-

rieren niedrig halten, indem sie zunächst gezielt ihre täglichen Desktop-Prozesse mobilisieren, was weniger Planung und auch ein niedrigeres Budget erfordert.

Gerätevielfalt

Eine weitere Herausforderung, aber auch Chance ist die Vielfalt mobiler Geräte auf dem Markt. In vielen Unternehmen nutzen die Mitarbeiter Smartphones verschiedener Anbieter mit unterschiedlichen Betriebssystemen. Eine Vereinheitlichung der Geräte ist für die meisten Unternehmen schon aus finanziellen Gründen, aber auch aus Gründen der Nutzerakzeptanz keine Option. Deshalb muss die IT-Abteilung wohl oder übel verschiedene Plattformen unterstützen.

Sichere Integration

Als nächstes stellen sich Fragen der zweckmäßigen und sicheren Integration der mobilen Geräte in die Unternehmens-IT: Wie wird der Netzwerkzugriff realisiert? Wie erfolgt die Anbindung an Unternehmensanwendungen? Ist ein Datenabgleich erforderlich? Wie können die Geräte zentral verwaltet werden? Wie kann ich bei Verlust oder Diebstahl eines Mobilgerätes Missbrauch verhindern? Auf Integrationskonzepte und Sicherheitsaspekte gehen wir unten in den Kapiteln 3 und 4 näher ein.

Mitarbeiterakzeptanz und Compliance

Wichtiger als die Technik aber ist der Anwender – er ist es schließlich, der unterstützt werden soll.

Die Herausforderung, die Mitarbeiter zur intendierten Nutzung der Unternehmensanwendungen zu motivieren, ihre Anwendungsbedürfnisse zu antizipieren und sie zur Einhaltung von entsprechenden Richtlinien zu bewegen, wird oft unterschätzt. Grundvoraussetzung für den Erfolg der Mobilisierung ist es, dass die mobilen Anwendungen zu den Arbeitsroutinen der Mitarbeiter passen und dass sie komfortabel und entsprechend der Nutzergewohnheiten zu bedienen sind.

Im Zusammenhang mit den Mitarbeitern fällt oft das Schlagwort von der „Consumerization" der IT: Mitarbeiter nutzen ihre privaten Geräte („personally owned devices", POD), Mail-Accounts oder Cloud-Services zunehmend auch für dienstliche Aufgaben, und sie äußern entsprechende Wünsche auch für die Unternehmens-IT. Laut einer Studie der Carnegie Mellon Universität in Pittsburgh, Pennsylvania, im Auftrag von McAfee (2011) nimmt nicht nur die Nutzung von Tablets und Smartphones in Unternehmen stark zu – ca. 63 Prozent dieser Geräte werden dabei sowohl beruflich als auch privat genutzt und ein Drittel der Nutzer speichert auch vertrauliche geschäftliche Daten auf dem Mobilgerät. CIOs sehen dies natürlich als Problem: Unternehmensdaten landen auf fremden Servern und auf Geräten, die man nicht selbst administrieren und sichern kann. Sie machen aber auch die Erfahrung, dass Verbote wenig helfen und Vorgaben umgangen werden, wenn die

Mitarbeiter das als notwendig ansehen. Consumerization kann kaum verhindert werden und ist andererseits auch ein Zeichen von Motivation – Unternehmen sollten also mit ihren Mitarbeitern nach optimalen Nutzungsmöglichkeiten auch von Consumer-Technologie suchen und dabei, wie bereits betont, ihre Anwendungsbedürfnisse antizipieren.

3 Mobile Konzepte und Integrationsstrategien

3.1 Grundsätzliche Überlegungen

Bevor ein Unternehmen den Ausbau mobiler Prozesse und die Integration geeigneter Mobilgeräte angeht, sind einige grundsätzliche Überlegungen notwendig, um sicherzustellen, dass man maximalen Nutzen aus der Mobilisierung zieht und dabei nicht an den falschen Stellen oder in die falsche Technologie investiert. Am Anfang jeder Mobilisierung steht eine Bestandsaufnahme: Wer hat schon welche mobilen Geräte im Einsatz? Welche meiner Mitarbeiter sind geeignete mobile Nutzer? In Frage kommen bei weitem nicht nur Außendienstler, sondern auch etwa solche Mitarbeiter, die viel Zeit in öffentlichen Verkehrsmitteln verbringen.

Am Anfang jeder Mobilisierung steht eine Bestandsaufnahme.

Nötig sind des Weiteren Überlegungen dazu, welche Device-Strategie zu den Zielen und Möglichkeiten des Unternehmens passt, welche mobilen Applikationen benötigt werden, wie tief die Mobilgeräte in die eigene IT-Infrastruktur integriert werden sollen und ob eine Hosting-Lösung oder eine selbst betriebene Plattform die bessere Wahl ist. Die jeweilige Entscheidung wird nicht nur von den Vor- und Nachteilen einzelner Konzepte, sondern vor allem auch von den verfügbaren Ressourcen eines Unternehmens (Budget, eigene IT-Abteilung, Know-how, Manpower) abhängen. Angesichts der rasanten Entwicklung mobiler Technologien sollten allerdings Bestandsaufnahme und strategische Überlegungen auch nicht zu übermäßigen Verzögerungen führen und damit den Erfolg des Projektes gefährden.

Schnelle Ergebnisse durch Desktop-Mobilisierung

Nach der bereits erwähnten PAC / Berlecon-Studie vom April 2011 haben zwei Drittel der deutschen Unternehmen keine langfristige Mobilstrategie. Grund sind (neben den gerade beschriebenen Herausforderungen) nicht zuletzt Bugdet-Fragen: Fast die Hälfte der befragten CIOs konnte kein Budget für mobile Technologien beziffern, die meisten anderen nur ein sehr begrenztes. Auch aus diesem Grund empfiehlt Cortado, in einem solchen Fall mit der Mobilisierung häufig genutzter Desktop-Prozesse zu beginnen – darauf wird in diesem Kapitel auch der Schwerpunkt liegen.

Mit der Mobilisierung typischer täglicher Arbeitsabläufe und Aktionen lassen sich – abhängig von der genutzten Technologie – ohne große Investitionen und mit verhältnismäßig geringem Aufwand sofortige Produktivitätssteigerungen erzielen. Zum Beispiel ergibt eine ROI-Betrachtung des Cortado Corporate Server, dass sich der Einsatz dieser Plattform durch Produktivitätssteigerungen und Prozessoptimierungen bereits nach 24 Tagen rentiert (selbst wenn direkte Einsparungen gegenüber Notebooks etwa bei WLAN- und Infrastrukturkosten, Support und Versicherung gar nicht einbezogen werden). Schnelle und nachweisbare Nutzwerte sind auch hilfreich bei späteren Budgetverhandlungen für umfangreichere Projekte. Zudem können so frühzeitig Erfahrungen gesammelt und Möglichkeiten ausgelotet werden, die der Mobilisierung weiterer Prozesse zugute kommen.

3.2 Device-Strategie

Unterstützung der wichtigsten Plattformen

Die erste Frage im Hinblick auf die Device-Strategie richtet sich auf die Alternative „private Geräte vs. unternehmenseigene Geräte“. Der Ansatz Bring-Your-Own-Computer (BYOC) ist für Unternehmen vergleichsweise kostengünstig, bringt aber ein deutliches Mehr an Komplexität mit sich. Dennoch sollte die gewählte Device-Strategie im Regelfall darauf abzielen, mindestens die wichtigsten Plattformen (Android, iOS, BlackBerry) zu unterstützen. Grundsätzlich ist auch im Unternehmenseinsatz eine gewisse Gerätevielfalt zu begrüßen: Viele Mitarbeiter bevorzugen ein bestimmtes Mobilgerät, dessen Bedienung sie gut beherrschen, oder besitzen bereits ein geeignetes Gerät (Akzeptanz). Zudem eignen sich Mobilgeräte durch ihre unterschiedliche Ausstattung zum Teil für verschiedene Einsatzzwecke verschieden gut, und oft gibt es auch regionale Unterschiede in bestimmten Features oder Verbreitung. Technisch ist die Nutzung heterogener Mobilgeräte heute kein Problem mehr: Der Cortado Corporate Server zum Beispiel bindet nicht nur Geräte unterschiedlicher Plattformen sicher in die IT ein, sondern passt sich in der Bedienung auch dem jeweiligen mobilen Gerät an und nutzt seine spezifischen Fähigkeiten und lokalen Ressourcen.

Der Cortado Corporate Server bindet Geräte unterschiedlicher Plattformen sicher in die Unternehmens-IT ein.

Mobile Device Management

Allerdings bietet derzeit nur RIM beim BlackBerry bereits einigermaßen umfangreiche Möglichkeiten für eine zentrale Geräteverwaltung. Bei Google und Apple (ebenso wie bei Microsoft) lassen die Administrationsmöglichkeiten diesbezüglich noch zu wünschen übrig, weshalb etwa PAC und die Fraunhofer ESK (2011) bei diesen Plattformen zum Einsatz zusätzlicher Mobile-Device-Management-Lösungen raten. Bevor Unternehmen allerdings beginnen, die Fülle am Markt befindlicher

MDM-Lösungen mit ihren sehr unterschiedlichen Funktionsumfängen (AetherPal, AirWatch, BoxTone, CommonTime, Excitor, FancyFon, Good Technology, InnoPath, Juniper Networks, McAfee, MobileIron, Motorola, Odyssey, Sybase, Symantec, Tangoe, Zenprise …) zu analysieren, sollten sie erwägen, ob nicht Microsoft Exchange mit den durchaus leistungsfähigen Konfigurations- und Sicherheitswerkzeugen von ActiveSync ihren Ansprüchen bereits genügt. Da viele Unternehmen ohnehin Microsoft Exchange einsetzen, ist dies in vielen Fällen die günstigste Lösung für das Mobile Device Management.

Tablets im Unternehmenseinsatz

Angesichts des starken Wachstums im Tablet-Markt sollten Unternehmen auch den Einsatz von Tablets in Erwägung ziehen. Dabei geht es nicht um die Frage „Smartphone oder Tablet?“, sondern um die Eignung verschiedener Geräteklassen für unterschiedliche Aufgaben. Zum Beispiel fördert der gemeinsame Blick auf das Tablet-Display die persönliche Interaktion – ideal im Vertriebsgespräch. Tablets können überall dort eingesetzt werden, wo PCs oder Notebooks zu groß oder zu sperrig und Smartphones schon zu klein sind. Dokumente etwa lassen sich mit Tablets wesentlich besser lesen und handhaben als mit Smartphones. Tablets sind vergleichsweise günstig, leicht und schnell einsatzbereit, bieten eine hohe Leistung, lange Akkulaufzeiten und einfache Bedienung und sind nahezu wartungsfrei. Außerdem können sie auf ein riesiges Ökosystem von kostengünstigen Apps zugreifen – und sie genießen nicht zuletzt ein ausgezeichnetes Image.

Aufgrund ihrer einzigartigen Möglichkeiten sind Tablets eine wertvolle Ergänzung zu Notebooks und Smartphones.

3.3 Mobile Desktop-Konzepte

Ziel der Desktop-Mobilisierung ist es, Funktionen und Daten, welche Mitarbeiter auf ihren Firmen-PCs nutzen, auch auf Mobilgeräten zur Verfügung zu stellen. Dies kann auf verschiedenem Wege passieren. Bei Notebooks etwa ist es immer noch üblich, die Desktop-Ausstattung zu replizieren, also benötigte Anwendungen direkt auf dem Gerät zu installieren.

Auch bei Tablets oder Smartphones ist das grundsätzlich möglich – bei einigen Geräten sind zum Beispiel Office-Anwendungen bereits vorinstalliert. Allerdings sind die Möglichkeiten limitiert: durch Ausstattung und Ressourcen der Geräte, durch sicherheitsbedingte Einschränkungen – lokale Apps können oft nur eingeschränkt miteinander interagieren und auf das Dateisystem zugreifen (Sandbox-Prinzip) – oder auch durch die Tatsache, dass die gewünschten Funktionen auf verschiedenen Geräten ganz unterschiedlich (oder auch gar nicht) implementiert sind. Gesicherte Netzwerkzugriffe über VPN sind mit Smartphones zwar möglich, gewohnte Netzwerkfunktionen wie Laufwerks-Mapping oder Drucken sind aber

dann auf den Mobilgeräten nicht verfügbar. Inhalte wären nur über Intranet-Seiten des Unternehmens (z.B. Microsoft Sharepoint) zugänglich. Zwar könnten benötigte Daten (mit mehr oder weniger Einschränkungen) auch lokal auf den Mobilgeräten gespeichert sein. Das wäre allerdings ebenfalls mit erheblichen Problemen verbunden – Stichworte sind hier vor allem Datenabgleich und Datensicherheit, insbesondere die Absicherung gegen Missbrauch bei Verlust des Gerätes.

Offene Konzepte realisieren die Datensicherheit über lokale Verschlüsselung und die Integration in die IT.

Daher sind Ansätze vorzuziehen, bei denen das Smartphone per Mobilfunk auf extern bereitgestellte Desktop-Funktionen bzw. Ressourcen zugreift. Insbesondere bei einer intendierten gleichzeitigen Nutzung für private und dienstliche Zwecke gibt es dafür zwei grundsätzlich verschiedene Herangehensweisen: geschlossene Containerlösungen, zum Beispiel Remote-Desktop- bzw. Virtual Desktop-Infrastrukturen, oder offene Konzepte, zum Beispiel Cortados Ansatz des Desktop als mobile App. Geschlossenen Konzepten ist gemeinsam, dass sie die Unternehmensanwendungen von den übrigen Anwendungen auf dem Mobilgerät isolieren und sie sozusagen in einen Container „einsperren“, um so eine Gefährdung vertraulicher Daten durch die auch private Nutzung des Gerätes auszuschließen. Offene Konzepte dagegen verzichten auf diese Einschränkungen und realisieren die Datensicherheit über lokale Verschlüsselung und die Integration in die IT.

3.3.1 Geschlossene Lösungen: Der Desktop im Container

Remote-Desktop- und Virtual-Desktop-Lösungen haben sich beim stationären Computing im Unternehmensumfeld vielfach bewährt. Ihr Grundprinzip ist das des Server-based Computings: Anwendungen laufen nicht lokal auf dem Gerät, das der Benutzer bedient, sondern auf einem zentralen Server. Das Endgerät – der Client – muss im Prinzip lediglich Ein- und Ausgaben von Daten übertragen können und deshalb auch nicht sehr leistungsfähig sein (vgl. sogenannte „Thin Clients“). Beim Remote Desktop wird eine komplette Desktop-Umgebung auf diese Weise genutzt, wobei spezielle Remote-Display-Protokolle (RDP, PC-over-IP, ICA HDX) zur Anwendung kommen. Heute ist vor allem die sogenannte Desktop-Virtualisierung gebräuchlich, wobei die Desktop-Umgebung samt Rechnerressourcen, Betriebssystem und Anwendungen als virtuelle Maschinen bereitgestellt werden und jeder Remote-Nutzer daher auf seine eigene (virtuelle) Systemumgebung zugreift. Gerade wenn Unternehmen bereits Lösungen für die Desktop-Virtualisierung im Einsatz haben, scheint es nahezuliegen, diese auch für die Anbindung von Tablets oder Smartphones zu nutzen. Theoretisch steht damit auf dem Mobilgerät die Benutzeroberfläche eines klassischen Desktops mit sämtlichen Funktionen zur Verfügung. In der Praxis allerdings kollidieren dabei zwei völlig unterschiedliche Nutzungsphilosophien. Bei klassischen PCs stehen die intensive Bearbeitung von

Dokumenten mit oft komplexen Funktionen im Vordergrund; ihre Bedienung ist an eine große Displayfläche und die Nutzung von Tastatur und Maus angepasst. Tablets und Smartphones sind dagegen auf Mobilität und einfache Bedienung ausgerichtet; wichtigstes Eingabemedium ist der Touchscreen. Für die Bedienung klassischer Desktop-Anwendungen sind diese Geräte wenig geeignet und können dabei auch ihre Vorteile nicht ausspielen. Außerdem können die Desktop-Anwendungen nicht in lokale Apps auf dem Mobilgerät integriert werden, und es stehen weder MDM-Funktionen noch gerätespezifische Sicherheitsfeatures zur Verfügung. Nicht zuletzt erfordert ihre Nutzung aufgrund der zu übertragenden Datenmengen recht hohe Bandbreiten und setzt stets eine einigermaßen stabile Internetanbindung voraus, was bei schwankender Netzabdeckung in vielen Gebieten (Stichwort „Funkloch“) zu Problemen führt.

Ein anderer geschlossener Ansatz vermeidet einige dieser Nachteile und versucht Funktionalität und Bedienung an die Eigenheiten von Smartphones anzupassen: Anbieter dieses Ansatzes realisieren Geschäftsanwendungen als Anwendungen direkt auf dem Mobilgerät selbst (mit entsprechendem Zugriff aufs Backend), sperren aber aus Sicherheitsgründen die geschäftlichen Applikationen und Daten in einen separaten Bereich ein („Corporate Bubble“). Dieser Bereich ist nach dem „Sandkasten“-Prinzip von sämtlichen anderen Anwendungen auf dem Gerät komplett abgeschirmt. Interaktionen mit lokalen Apps oder Ressourcen außerhalb der Unternehmenskapsel sind unmöglich. Der Ansatz wird bei vielen Anbietern ergänzt durch Management-Funktionen für die mobilen Geräte, darunter auch die Möglichkeit zum zentral gesteuerten Löschen der Geschäftsdaten etwa bei Verlust oder Diebstahl des Smartphones („Remote Wipe“). Aber auch dieses Konzept hat gravierende Nachteile. Zugriff auf Dateien als wesentlicher Bestandteil der täglichen Arbeit wird von diesen Anbietern weitgehend ignoriert. Vor allem fehlt die Möglichkeit, den Funktionsumfang des Gerätes durch Apps zu erweitern und individuell an den eigenen Bedarf anzupassen. Sollen mitgelieferte Anwendungen der Smartphones, zum Beispiel der E-Mail-Client, genutzt werden können, muss der Anbieter diese nachprogrammieren, so dass Neuerungen bei der Smartphone-Plattform nur teilweise und mit oft großen Verzögerungen genutzt werden können. Ein weiteres potenzielles Problem ist die weitgehende Abhängigkeit vom MDM-Anbieter in Bezug auf Sicherheitsaspekte – hier ist eine sorgfältige Prüfung des Anbieters und seines Sicherheitskonzeptes wichtig. Letztendlich ist vor allem fraglich, ob die durch die beschriebenen Einschränkungen erkaufte Sicherheit überhaupt erreicht wird: Wenn diese Einschränkungen die tägliche Arbeit beeinträchtigen, werden Nutzer nach Wegen suchen, sie zu umgehen– und sie werden diese Wege finden (vgl. Kap 4.2).

In der Kapsel eingesperrte Anwender können nur die Funktionen nutzen, die der Anbieter bereitstellt.

3.3.2 Die offene Lösung: Der Desktop als App

Aus diesem Grund sind offene Lösungen, die auf das Einsperren geschäftlicher Anwendungen und Daten in einen Container verzichten, deshalb nicht weniger sicher als geschlossene Konzepte – ganz im Gegenteil (siehe unten Kapitel 4). Eine solche offene Lösung ist der „Desktop als App" – das Zusammenspiel einer speziellen App auf dem Mobilgerät, die dem Nutzer Zugang zu den wesentlichen Desktop-Prozessen verschafft, mit einer mehr oder weniger direkt in die Unternehmens-IT integrierten Server-Komponente. Letztere stellt nicht den kompletten PC-Desktop, sondern ausgewählte Desktop-Funktionen – z.B. Dokumentenzugriff und -ablage, Dateiversand per E-Mail, Dateikonvertierung (PDF, ZIP), Datenbankberichte, Drucken, Faxen etc. – als „virtuelle Desktop-Prozesse" zur Verfügung. Dieses Konzept, auf das die Lösungen von Cortado zurückgreifen, nutzt die wesentlichen Vorteile der bisher beschriebenen Konzepte und vermeidet ihre Nachteile:

Der Desktop als App macht ausgewählte Unternehmensressourcen in einer für die Nutzung auf einem Smartphone oder Tablet optimierten Form zugänglich.

- Volle Integration in die IT-Infrastruktur inkl. Berechtigungskonzept
- Zugriff auf Dateisystem und Netzwerkdrucker
- Geräteoptimierte Bedienung
- Online-Speicherung von Daten
- Online Preview von Dateien
- Offline-Speicherung und Bearbeitung von Dokumenten mit „Bordmitteln"
- Möglichkeit je Nutzer Rechte flexibel managen/einschränken zu können
- Nutzung lokaler Ressourcen (z. B. Drucker, Kameras, Adressbuch)

Der Desktop als App ermöglicht eine echte Integration in die individuelle IT-Landschaft des Unternehmens einschließlich verwendeter Richtlinien und Berechtigungskonzepte, anstatt lediglich die Infrastruktur um zusätzlich angebundene Komponenten zu erweitern. Die Server-Komponente (z.B. der Cortado Corporate Server) übernimmt im Unternehmen die Integration in das Microsoft Active Directory (und ggfls. E-Directory). Sie greift für den mobilen Client auf das Dateisystem zu, so dass dieser die gewohnte Verzeichnisstruktur inkl. Laufwerksnamen und -buchstaben darstellt, und sie übernimmt die Kommunikation mit weiteren Komponenten im Backend wie beispielsweise Netzwerkdruckern, Datenbankreports und dem Faxsystem. Dabei agiert der Benutzer mit seinen Rechten, wie sie im Active Directory definiert sind. Bestimmte Szenarien können nur auf diese Weise ohne Medienbrüche oder späteres Abarbeiten im Backoffice abgebildet werden. Will zum Beispiel ein Kollege im Außendienst Informationen erfassen, kann er das mit Zugriff auf das Unternehmensnetzwerk direkt in dem Dokument tun, in das diese Informationen gehören. Ohne Integration in das Unternehmens-Netz müsste er die Daten doppelt erfassen – oft auf Papier – und sie später an seinem Arbeitsplatz einarbeiten.

Zum anderen können – im Gegensatz zur Desktop-Virtualisierung – die Benutzeroberfläche der mobilen App an das mobile Gerät und auch an die Eigenheiten der jeweiligen Plattform angepasst und so die individuellen Vorteile des verwendeten Gerätes optimal genutzt werden. Cortado stellt dafür Clients für die Betriebssysteme Google Android, Apple iOS und BlackBerry OS zur Verfügung. Der Client kann auch andere Apps auf dem Gerät aufrufen (etwa Quick Office auf Android oder Keynote auf dem iPad) oder von ihnen aufgerufen werden. Damit ist es dem mobilen Nutzer z. B. möglich, einen Mail-Anhang direkt im Unternehmensnetzwerk abzulegen oder auch ein Dokument aus dem Netzwerk direkt auf seinem Gerät zu bearbeiten. Beim Herunterladen von Dokumenten werden diese komprimiert, um das übertragene Datenvolumen zu reduzieren und Kosten zu sparen. Dateioperationen wiederum sind auf allen Geräten einheitlich möglich, obwohl iOS intern dabei nach ganz anderen, restriktiveren Prinzipien arbeitet als Android und BlackBerry OS.

4 Sicherheit

Die IT-Sicherheit wird durch Entwicklungen wie Cloud-Computing, Consumerization und den zunehmenden Einsatz mobiler Geräte vor große Herausforderungen gestellt. Wie bereits angedeutet, reicht es nicht, technische Sicherheitsmaßnahmen zu ergreifen, wenn nicht gleichzeitig der Anwender und seine Nutzungsgewohnheiten berücksichtigt werden. Die sicherste Lösung nützt nichts, wenn der Anwender sie umgeht und eine bequemere wählt, bei der vertrauliche Daten in unsicheren Systemen landen. Dennoch ist es natürlich unbedingt notwendig, die wesentlichen Angriffspunkte der mobilen IT-Infrastruktur auch technisch abzusichern: das Mobilgerät selbst, mobile Applikationen und Datenübertragung sowie die Integration ins Backend.

Cloud-Computing, Consumerization und der Einsatz mobiler Geräte stellt die IT-Sicherheit vor große Herausforderungen.

4.1 Mobilgeräte absichern

Mobile Geräte können verloren gehen oder gestohlen werden. Für einen solchen Fall muss sichergestellt sein, dass vertrauliche Unternehmensdaten nicht in die falschen Hände fallen. Die Geräte selbst bieten dafür unterschiedliche Möglichkeiten, um die definierten Sicherheitsrichtlinien eines Unternehmens zu unterstützen. Wichtigste Vorkehrung ist die Nutzung eines sicheren Kennworts – dies ist mit jedem Gerät möglich. Ist der Zugang zum Gerät auf diese Weise abgesichert, so gewinnt das Unternehmen zumindest Zeit für weitere Maßnahmen. Darüber hinaus ist eine Verschlüsselung der gespeicherten Daten ratsam. Apples iOS 4.x bietet ein durchaus ausgefeiltes Sicherheitssystem mit einer auf einer Hierarchie von Schlüsseln basierenden Verschlüsselung, komplexen alphanumerischen Pass-

wörtern und automatischer Selbstlöschung bei wiederholten falschen Eingaben. Allerdings wird von diesen Möglichkeiten (mit Ausnahme von Apples Mail-Client) noch kaum Gebrauch gemacht. Es ist daher wichtig, darauf zu achten, dass eventuell eingesetzte mobile Apps, so wie es auch die Cortado-Lösung tut, ihre Daten gemäß der Apple-Sicherheitsarchitektur vollständig verschlüsseln.

Noch immer erfreut sich zudem der sogenannte Jailbreak großer Beliebtheit, mit dem die Software-Sperre des iPhone umgangen wird, so dass der Nutzer Anwendungen aus anderen Quellen als dem App Store installieren kann. Anfang 2011 demonstrierte das Fraunhofer-Institut, dass sich ein Angreifer bei einem aktuellen iOS mit installiertem Jailbreak innerhalb von nur sechs Minuten und ohne besondere Fachkenntnisse Zugang zu Passwörtern für E-Mail, W-Lan und VPN verschaffen kann, auch bei Geräten mit hohen Sicherheitseinstellungen. Bei Verlust eines iPhones sollte ein Unternehmen daher umgehend reagieren, da gerade über den E-Mail-Account oft zahlreiche weitere Passwörter erbeutet werden können. Das Passwort der Cortado-Lösung kann allerdings auch beim Jailbreak nicht in die falschen Hände geraten, weil Cortado Kennwörter nicht lokal speichert.

Das Passwort der Cortado-Lösung kann beim Jailbreak nicht in die falschen Hände geraten, weil Cortado Kennwörter nicht lokal speichert.

BlackBerry-Nutzern steht schon länger eine hohe Verschlüsselung auf Betriebssystemebene zur Verfügung, während Android erst seit der Version 3.0 eine solche mitbringt. BlackBerry offeriert mit dem BlackBerry Enterprise Service (BES) auch die umfangreichsten Möglichkeiten, Sicherheitsrichtlinien umzusetzen. Google bietet dafür die Google Apps Device Policy Administration an, Apple das Apple Mobile Device Management, welches allerdings nur durch die Nutzung von Third-Party-Zusatzsoftware zur Verfügung steht. Für alle drei Plattformen sind inzwischen insbesondere Funktionen zum Fernzugriff auf die Geräte verfügbar, um bei Verlust Zugangscodes zurückzusetzen und Daten zu löschen.

Zusätzliche Lösungen zum Mobile Device Management bieten plattformübergreifend ebenfalls diese Möglichkeit, zum Beispiel Sybase Afaria, Good for Enterprise von Good Technologie oder AirWatch. Aber auch Microsoft Exchange Active Sync erlaubt bereits Remote Wipe, das Erzwingen der Geräteverschlüsselung sowie von Passwortrichtlinien wie beispielsweise von alphanumerischen Passwörtern ausreichender Komplexität.

4.2 Kommunikation und Applikationssicherheit

Die Datenübertragung zwischen Mobilgerät und Unternehmensnetzwerk sollte grundsätzlich verschlüsselt erfolgen. Bei erhöhten Sicherheitsanforderungen können vertrauliche Daten zusätzlich auch via VPN getunnelt werden. Android und

iOS unterstützen dafür Standard-VPN-Verbindungen, während BlackBerry einen proprietären VPN-Tunnel namens Mobile Data Service (MDS) nutzt. Anwendungen von offiziellen Partnern der RIM Alliance – zum Beispiel von Cortado – nutzen ebenfalls diesen sicheren Tunnel. Ansonsten erfolgt die Kommunikation zwischen Client und Server beim Cortado Corporate Server ausschließlich über HTTPS, eine Tunnelung über VPN oder die Nutzung von Zwei-Faktor-Authentifizierung ist optional möglich.

Auch bei der Integration der Mobilgeräte in die IT-Infrastruktur eines Unternehmens gilt es Sicherheitsaspekte zu beachten.

Geschlossene Lösungen scheitern am Anwender

Häufig werden Mobilgeräte sowohl für private als auch für dienstliche Zwecke genutzt. In diesen Fällen hat die IT-Abteilung kaum Kontrolle darüber, ob neben den mobilen Unternehmensapplikationen andere, potenziell unsichere oder bösartige Software installiert wird. Um auszuschließen, dass auf dem Mobilgerät selbst ein erfolgreicher Angriff auf die Unternehmens-App bzw. vertrauliche Daten stattfinden kann, setzen viele Unternehmen auf das „Einsperren“ ihrer Anwendung in einen Container (vgl. Kap. 3.3.1). Geschlossene Lösungen haben allerdings den Nachteil, dass sie nur funktionieren können, wenn sie gleichzeitig dem Nutzer den Komfort und sämtliche Funktionen bieten, die er benötigt. Neben den in Kap. 3.3.1 besprochenen Nachteilen fehlt dem Nutzer dabei insbesondere die Möglichkeit, auch offline – direkt auf dem Gerät – auf Dateien zuzugreifen. Dies ist aber in vielen Fällen gewünscht (bspw. wenn er Funktionen oder den Bedienkomfort bestimmter Apps nutzen möchte), wenn nicht sogar nötig, beispielsweise wenn er Dokumente im Flugzeug bearbeiten will oder sich bei der Präsentation beim Kunden nicht auf die Netzabdeckung vor Ort verlassen kann.

Wenn der Anwender so an die Grenzen seiner Unternehmensanwendungen stößt, wird er einen Weg aus dem Container finden. Er kann sich zum Beispiel Firmendokumente an die private E-Mail-Adresse senden oder sie mit Hilfe unsicherer Cloud-Dienste wie Dropbox auf das Gerät bringen. Dann landen vertrauliche Daten doch wieder in privaten E-Mail-Accounts, unsicheren Cloud-Services und unverschlüsselt auf den Geräten, wo sie dann auch dem Zugriff durch das MDM und jeder Nachvollziehbarkeit entzogen sind.

Jede Lösung muss sowohl in Bezug auf die gebotene technische Sicherheit als auch auf ihre Akzeptanz hin geprüft werden – optimal sind Lösungen, die beides vereinen.

Das Konzept von Cortado gestattet daher explizit die Nutzung lokaler Apps und ermöglicht die Offline-Verfügbarkeit von Dateien. Unabdingbare Voraussetzung dafür ist wie schon erwähnt die Nutzung der lokalen Verschlüsselungsfunktionen, die heute leider noch immer keine Selbstverständlichkeit ist. Das Beispiel zeigt, dass offene Konzepte, die solche Aktionen explizit erlauben und dafür sichere Wege anbieten, aufgrund ihrer höheren Flexibilität für den Nutzer letztlich sicherer sind als Container-Lösungen.

4.3 Sichere Integration ins Backend

Die verfügbaren Möglichkeiten einer Absicherung der Backend-Integration ist abhängig vom gewählten Integrationskonzept (siehe Kapitel 3). Die folgenden Prinzipien haben sich als besonders vorteilhaft erwiesen – insbesondere wenn das Verhältnis von **Funktionalität, Komfort und Sicherheit** beurteilt wird.

1. Integration ins Active Directory:

Eine möglichst vollständige Integration ins Active Directory ermöglicht es, sämtliche von einem Mobilgerät initiierten Prozesse ausschließlich als angemeldeter Benutzer und im Kontext seiner definierten Berechtigungen auszuführen.

Der Cortado Corporate Server erlaubt darüber hinaus auch noch weitere Festlegungen, zum Beispiel, welche Laufwerke, Ordner oder Netzwerkdrucker der jeweilige Anwender auch vom mobilen Gerät sehen kann, ob er Dateien im Unternehmensnetz löschen darf und ob der Up- und Download von Dateien für ihn erlaubt sein soll.

2. Zentrale Datenhaltung:

Die Datenhaltung auf dem mobilen Gerät sollte eingeschränkt werden. Dadurch verringern sich nicht nur das Risiko eines Datenverlustes und der Aufwand für die Synchronisation, sondern auch die Gefahr, dass Anwender unterwegs alte Dateiversionen nutzen. Deshalb sorgt die Cortado-Lösung für die sichere Verfügbarkeit der zentral im Unternehmensnetzwerk gespeicherten Daten für den mobilen Gebrauch und macht dadurch die dezentrale Datenhaltung auf dem Mobilgerät weitgehend überflüssig.

3. Möglichst wenig Ports öffnen:

Je nachdem, welche Systeme bzw. Applikationen mit dem Mobilgerät kommunizieren sollen, müssen Ports geöffnet werden, die zum Einfallstor für Angreifer werden können. Daher sollte eine Lösung gewählt werden, bei denen möglichst wenig Ports genutzt werden. Für die Cortado-Lösung z.B. muss nur ein einziger Port (443) geöffnet werden.

4. Spezielle Anforderungen:

Bei der Wahl einer Integrationslösung müssen eventuell bestehende besondere Sicherheitsanforderungen berücksichtigt werden, etwa die Unterstützung von Hochverfügbarkeit oder die Möglichkeit des Trackings von Geräten und des Auditings, also des Protokollierens der Nutzeraktivitäten auf den Systemen. Letzteres erhöht nicht nur Nachvollziehbarkeit und Sicherheit (z.B. durch frühzeitiges Erkennen eines Missbrauchs), sondern kann auch zur Kostensenkung beitragen (z.B. Druck-

kostenkontrolle). Eine andere, für viele nicht unwichtige Frage ist die nach den Datenschutzbedingungen der Plattformanbieter: Apple etwa behält sich in seinen AGBs vor, eine Reihe von Nutzerdaten zu erheben.

Es ist in jedem Fall empfehlenswert, bereits vor der Implementierung mobiler Prozesse eine konkrete Risiko- und Schwachstellenanalyse für das eigene Unternehmen durchzuführen. Dabei werden nicht nur mögliche Bedrohungen identifiziert, sondern auch die Ressourcen des Unternehmens daraufhin beurteilt, ob sie ausreichen, diesen Bedrohungen wirksam zu begegnen. Wer nicht selbst über das notwendige Know-how und Personal verfügt, sollte sich in jedem Fall Unterstützung von erfahrenen IT-Experten holen. Klar jedoch sollte eines sein: Vollständige Sicherheit gibt es nicht – jedes Unternehmen muss Risiken und Chancen, mögliche Sicherheitsbedrohungen, den Aufwand ihrer Abwehr und die zu erwartenden Vorteile durch mehr Produktivität und Flexibilität für sich abwägen.

Hauptniederlassung

Cortado AG
Alt-Moabit 91a/b
10559 Berlin, Germany

Tel.: +49 (0)30-39 49 31-0
Fax: +49 (0)30-39 49 31-99

E-Mail: info@team.cortado.de
www.cortado.de

USA (Ohio) Niederlassung

Cortado, Inc.
20006 Detroit Rd
Cleveland, OH 44146, USA

Tel: +1-440-331-8446
Fax: +1-303-942-7500

E-mail: info@cortado.team.com
www.cortado.com

Cortado, Inc. USA (Colorado) Niederlassung
7600 Grandview Avenue, Suite 200
Denver, CO 80002, USA

Tel.: +1-303-487-1302
ax: +1-303-942-7500

Cortado Pty Ltd. Australien Niederlassung
Level 20, The Zenith Centre, Tower A,
821 Pacific Highway
Chatswood, NSW 2067, Australien

Tel.: +61-(0)2-84 48 20 91

Cortado Japan Japan Niederlassung
B1 AIG building · 1-1-3 Marunouchi
Chiyoda-ku, Tokyo 100-0005

Tel.: +81-(0)3-52 88 53 80
Fa x: +81-(0)3-52 88 53 81

CORTADO
Business Class of Cloud Desktop Services

ThinPrint®
A Brand of CORTADO