Gesponsert von Acronis

IDC Multi-Client-Projekt | Executive Brief

MOBILE CONTENT MANAGEMENT IN DEUTSCHLAND 2014

File-Sharing & Synchronisation als Erfolgsfaktor für mobiles Arbeiten

IDC
Analyze the Future

Inhaltsverzeichnis

Autoren:
Ariane Mackenzie, Consulting Manager, European Telecommunications and Networking & Projektleiterin, IDC
Mark Alexander Schulte, Consultant & Projektleiter, IDC

MOBILE CONTENT MANAGEMENT IN DEUTSCHLAND 2014

Einleitung

Unternehmen sind derzeit an einem Punkt angelangt, an dem sie Mobilität nicht nur akzeptieren, sondern diese als Teil ihrer Firmenstrategie auch implementieren müssen. Dies wirkt sich entsprechend auf die drei wesentlichen Bereiche der Unternehmens-IT aus: Endgeräte, Applikationen und Daten. Während Endgeräte und Applikationen in den meisten Unternehmen bereits Teil der firmenweiten mobilen Strategie sind, wird das Teilen und Synchronisieren der Daten noch sehr individuell von einzelnen Mitarbeitern gehandhabt. 52 % der befragten Unternehmen geben in der von IDC durchgeführten Studie „Mobile Content Management in Deutschland 2014" an, dass sie partiell bereits File-Sharing- und Synchronisationslösungen in der ein oder anderen Form nutzen, die Hälfte davon räumt aber ein, dies ohne Wissen der IT zu tun. Das heißt, dass sich gerade in diesem sehr sensiblen Bereich, bei dem es um kritische Firmendaten geht, eine Schatten-IT herausbildet, die eine Kontrolle seitens der IT unmöglich macht.

Aus Mangel an firmenweiten Strategien behelfen sich die Mitarbeiter oft mit Lösungen aus dem privaten Umfeld. Fachbereiche verfolgen die gleichen Ziele wie ihre Kollegen aus der IT, nämlich sicheren Datenaustausch zwischen Mitarbeitern, Kunden und Partnern sowie sichere Synchronisation der Dokumente auf allen im Unternehmen eingesetzten mobilen Endgeräten. Ob eine Public oder Private Cloud oder eine On-Premise-Lösung als Bereitstellungsmodell gewählt wird: Das oberste Ziel für alle Bereiche ist es, die Sicherheit von Daten und Dokumenten zu gewährleisten, so das Fazit der aktuellen IDC-Studie.

Im Dezember 2013 befragte IDC zu dieser Thematik 238 IT- und Fachbereichsentscheider aus Unternehmen mit mehr als 100 Mitarbeitern. Die wichtigsten Trends werden im Folgenden zusammengefasst.

Trends und Entwicklungen in Deutschland

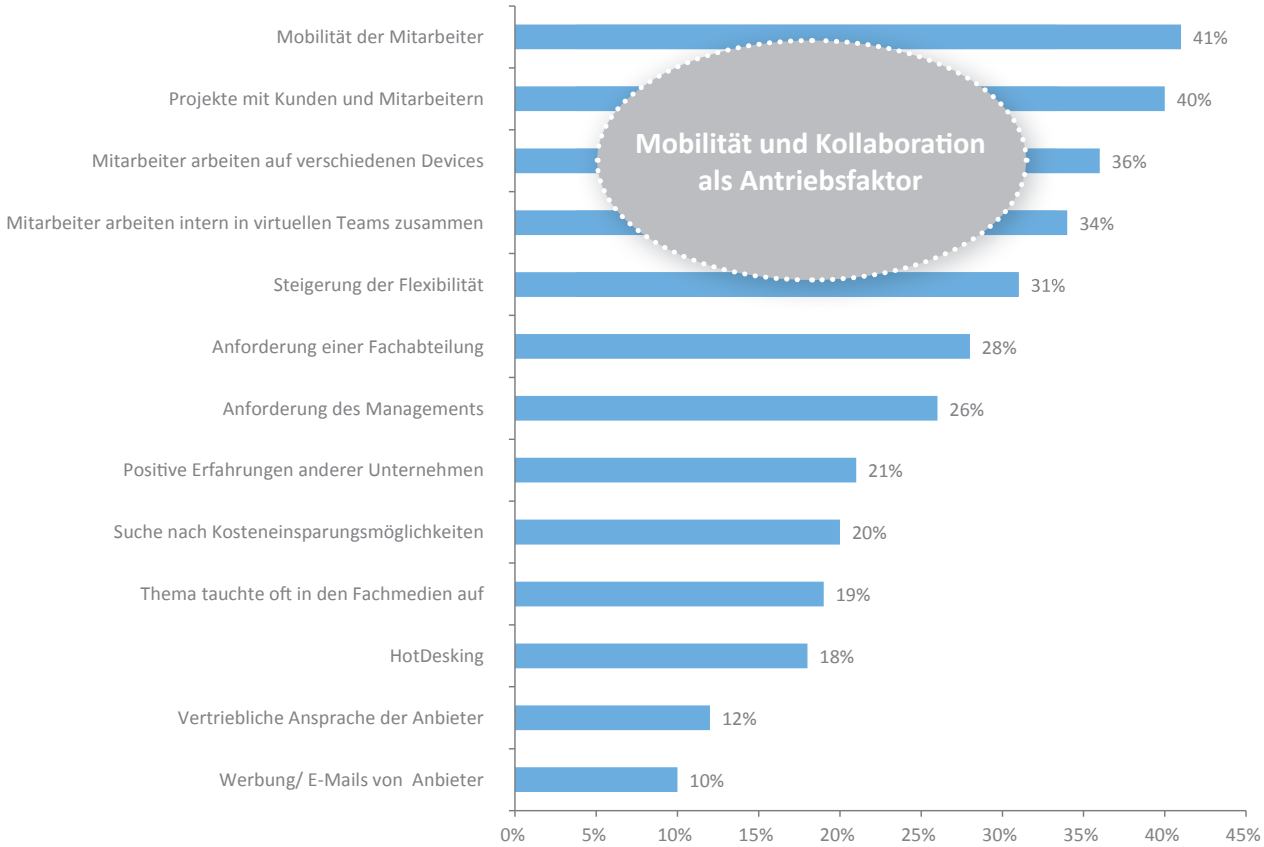
Unternehmen setzen Tools für mobiles und kollaboratives Arbeiten ein

Als Hauptgrund für die Überlegung, in File-Sharing- und Synchronisationslösungen zu investieren, wird von 41 % der Anwenderunternehmen angegeben, dass Mitarbeiter sehr mobil sind und immer und überall Zugriff zu ihren Dokumenten brauchen. Zudem stellen auch Projekte mit Kunden und Partnern und das Zusammenarbeiten in virtuellen Teams wichtige Beweggründe für die Evaluierung von File-Sharing- und Synchronisationslösungen dar.

Antriebsfaktoren für die Implementierung von File-Sharing- und Synchronisationslösungen

Was war für Ihr Unternehmen der Ausgangspunkt, sich mit dem Thema File-Sharing und Synchronisation zu beschäftigen?

ABBILDUNG 1



Quelle: IDC, 2014

n = 238, Alle, Mehrfachnennungen

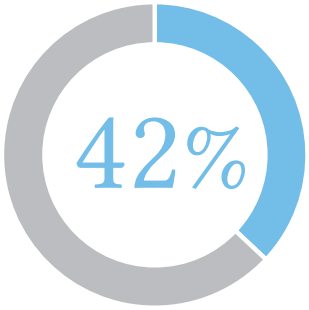
Somit drehen sich die meistgenannten Pushfaktoren bei diesem Thema um Kollaboration, Mobilität und die damit verbundene Flexibilität. In den meisten Fällen besteht in den Unternehmen ein konkreter Bedarf; extern durch Fachmedien, Werbung und allgemeine Informationen der Anbieter generiertes Interesse bietet nur einen untergeordneten Anreiz, sich mit dem Thema auseinanderzusetzen.

Teilen und Synchronisieren von Dokumenten: Neue Lösungen sind nötig

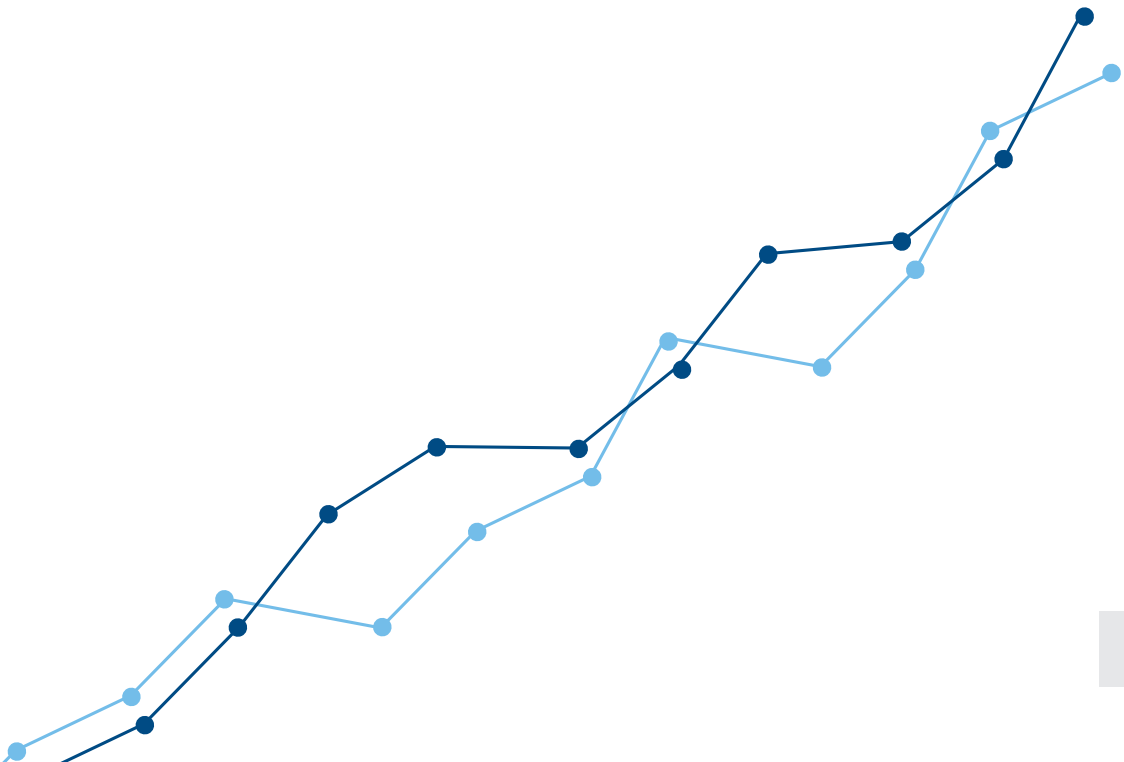
Laut Umfrage benutzen 74 % aller Unternehmen E-Mails zum Teilen und Verschicken von Dokumenten; 55 % nutzen E-Mails zum Synchronisieren der Dokumente auf verschiedenen Endgeräten. Allerdings geben die Befragten an, dass sich diese Zahl in den nächsten 12 Monaten zu Gunsten von File-Sharing- und Synchronisationslösungen drastisch verringern wird. Mitarbeiter helfen sich aus Mangel an firmenumfassenden Lösungen selbst – E-Mail und die klassischen externen Devices, wie USB-Stick oder externe Festplatte, sind die gängigsten Mittel, doch auch File-Sharing- und Synchronisationslösungen aus dem privaten Umfeld werden von 25 % der Befragten genannt. Sowohl die IT als auch die Fachbereiche sind sich bewusst, dass File-Sharing- und Synchronisationslösungen auf Unternehmensebene implementiert werden müssen, um alle unsicheren Insellösungen zu vermeiden. Immerhin geben 42 % der Befragten an, dass sie planen, in den nächsten 12 Monaten eine Enterprise-File-Sharing- und Synchronisationslösung zu nutzen.

Stabil hingegen bleibt der Zugriff auf Daten über das Firmen-VPN. Die Hälfte der Anwenderunternehmen stellt diese Methode als Zugang bereit und hat nicht vor, dies in den nächsten 12 Monaten zu ändern. Ein starker Rückgang ist bei den externen Speicherquellen zu sehen: USB-Sticks, CD-ROMs oder externe Festplatten sollen den Anwendern zufolge immer weniger im Unternehmen verwendet werden.

FAKTEN

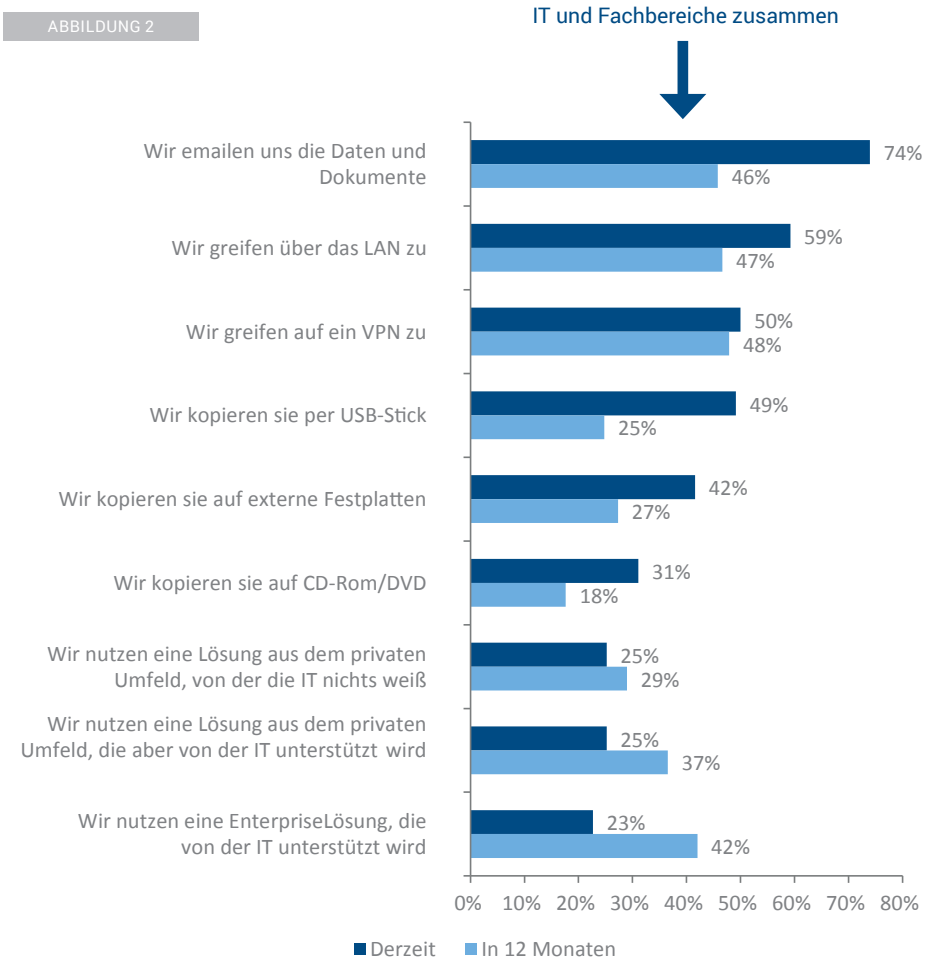


der Befragten geben an, dass sie planen, in den nächsten 12 Monaten eine Enterprise-File-Sharing- und Synchronisationslösung zu nutzen.



Wie teilen die Mitarbeiter derzeit Dokumente und wie wird dies in 12 Monaten erfolgen?

ABBILDUNG 2



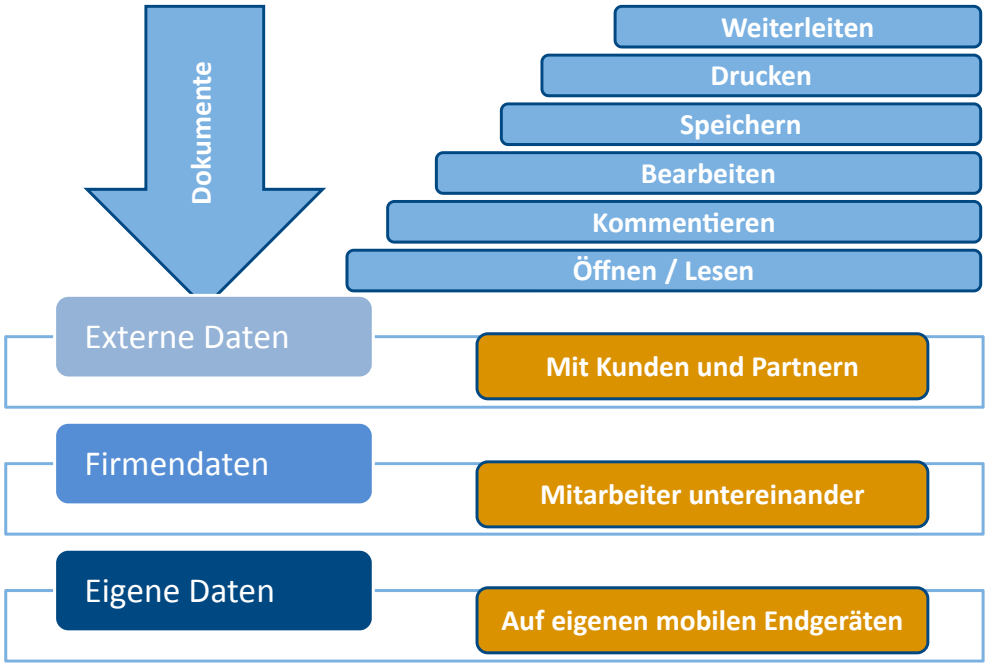
Quelle: IDC, 2014
n = 238, Alle, Mehrfachnennungen

Eine weitere Herausforderung beim Verschicken von Content über E-Mail ist das Speichern der Dokumente auf dem eigenen Desktop oder Laptop. 63 % der Befragten geben an, dass der zu teilende Content lokal abgelegt wird. Gerade dieses lokale Speichern von Daten führt verstärkt zu Problemen mit der Versionierung und gleichzeitigen Bearbeitung von Dokumenten. Anwender haben in der Befragung angegeben, dass genau dies das Hauptproblem in Bezug auf Kollaboration ist. Die Tatsache, dass verschiedene Versionen eines Dokuments im Umlauf sind, merken die Mitarbeiter oft zu spät. Durch die Bereitstellung klar definierter Kollaborations-Tools kann somit der Mehraufwand bei ungewollt gleichzeitiger Bearbeitung von Dokumenten minimiert und die Effizienz gesteigert werden.

Zugriff auf File-Sharing- und Synchronisationslösungen wird nach Aufgaben vergeben, nicht nach Hierarchie

Inwieweit Mitarbeiter Zugang zu den verschiedenen File-Sharing- und Synchronisationslösungen erhalten, zeigen die folgenden Ergebnisse. Aktuell geben 33 % der Unternehmen, die bereits eine Lösung implementiert haben, jedem Mitarbeiter Zugriff. Nicht so wichtig scheint die hierarchische Struktur für die Zugangsregelungen zu sein: Nur 16 % geben selektiv Teamleitern und Abteilungsleitern Zugang zu File-Sharing- und Synchronisationslösungen. Dies legt den Schluss nah, dass hierzulande die Unternehmen unabhängig von der jeweiligen Position ihren Mitarbeitern Zugriff zu File-Sharing- und Synchronisationslösungen geben. Die Entscheidung über den Zugang hängt vielmehr von der Zugehörigkeit zu virtuellen Teams oder anderen aufgabenorientierten Gruppen ab.

Bearbeitungsebenen eines Content Management-Tools



Source: IDC, 2014

Der Zugang zu Dokumenten muss auf zwei Ebenen definiert werden: einerseits auf Mitarbeiterebene, andererseits aber auch auf der Dokumenten- oder Ordnerebene. Für beide Ebenen müssen Richtlinien erstellt werden, was innerhalb einer Gruppe oder eines Dokumentes erlaubt ist. So kann sich der Zugang auf das Lesen und Kommentieren eines Dokumentes beschränken oder dem Benutzer das Bearbeiten, Speichern und Weiterleiten erlauben.

Datensicherheit muss bei allen Bereitstellungsmodellen adressiert werden

Sind einerseits Kollaboration und Mobilität und die damit verbundene Flexibilität und Steigerung der Effizienz die größten Treiber für das Implementieren einer File-Sharing- und Synchronisationslösung, so ist die Angst um die Sicherheit der Daten der größte Hemmfaktor dafür, egal ob nun Diebstahl und Missbrauch der Daten oder Kontrollverlust befürchtet werden.

Anwender sind sich aber auch bewusst, dass die derzeitige Situation ebenfalls nicht sicher ist und eine Implementierung einer File-Sharing- und Synchronisationslösungen in jedem Fall eine Verbesserung der Ist-Situation darstellen würde. Sowohl IT als auch Fachbereiche sind sich einig, dass Nichtstun das Entstehen einer Schatten-IT und damit noch mehr Sicherheitsrisiken mit sich bringen würde.

Auf die Fragen nach dem bevorzugten Bereitstellungsmodell geben 51 % der Befragten an, eine Private Cloud zu nutzen, weitere 26 % ziehen eine Public Cloud dafür in Erwägung. Vor allem ist die lokale Präsenz der Datenzentren bei vielen Unternehmen essenziell: 43 % der Anwender geben an, dass sich das Datenzentrum auf jeden Fall in Deutschland befinden muss. Weitere 18 % halten ein deutsches Datenzentrum für wünschenswert, aber nicht zwingend notwendig, und 19 % wollen es auf jeden Fall in Europa wissen.

In Bezug auf Sicherheitsmaßnahmen von File-Sharing- und Synchronisationslösungsanbietern vertrauen die deutschen Unternehmen auf zertifizierte Sicherheitsstandards. Hierbei sind der TÜV (68 %) und die ISO-Zertifizierungen (50 % für ISO 2000 und 46 % für ISO 27001) am bekanntesten.

Neben File-Sharing- und Synchronisationslösungen aus der Private oder Public Cloud oder einer On-Premise-Lösung, stellen Anbieter verschiedenste Bereitstellungsmodelle zur Verfügung, zwischen denen Unternehmen wählen können. Welches Model am besten zur Firmenkultur und in die IT-Landschaft passt, muss individuell evaluiert werden.

Fazit

Mit File-Sharing- und Synchronisationslösungen wollen deutsche Unternehmen die Datensicherheit verbessern und eine Strategie implementieren, die firmenweiten Zugriff auf und Austausch von Daten ermöglicht. Vor dem Hintergrund der zunehmenden Mobilität und einer wachsenden Zahl an mobilen Endgeräten steht dabei die Verbesserung der Effizienz im Fokus. Den Mitarbeitern muss ermöglicht werden, strukturiert in virtuellen Teams zu arbeiten, ohne dass sie Konflikte mit der Versionierung von Dokumenten riskieren. Gleichzeitig benötigen sie über verschiedene Endgeräte Zugriff auf alle Firmendaten, ohne diese lokal speichern zu müssen. Genau dieser Aspekt ist bei Verlust oder Diebstahl von Endgeräten wichtig, da lokal abgelegte Daten für die IT weder kontrollierbar noch zugänglich sind. Nach Meinung von IDC haben IT und Fachbereiche das gleiche Ziel: Nämlich sicheren Datenaustausch. Allerdings mangelt es den Fachbereichen oft an Geduld, auf eine unternehmensweite Implementierung von File-Sharing- und Synchronisationslösungen seitens der IT zu warten, weswegen sie sich mit Lösungen aus dem privaten Umfeld behelfen. Um dem entgegenzuwirken, sollten IT Abteilungen die Bedürfnisse der Benutzer adressieren und pro-aktiv eine firmenweite Lösung finden.

Die verschiedenen Bereitstellungsmodelle der Anbieter für File-Sharing- und Synchronisationslösungen müssen genau evaluiert werden. Wichtig dabei sind auch TÜV- oder ISO-Zertifizierungen der Produkte sowie Zugangsverschlüsselungen und Authentifizierungen auf allen Ebenen: Authentifizierung der Benutzer, der Endgeräte und der Daten.

Empfehlungen

So transformieren Sie Ihr Content Management

Die Sicherheit der Daten ist den Unternehmen in Deutschland überaus wichtig. IDC ist der Überzeugung, dass ein mehrstufiger Prozess implementiert werden sollte, der das Teilen und Synchronisieren von Daten und Dokumenten sicherer macht. Dieser Prozess benötigt Zeit, da die gewohnten Arbeitsweisen geändert werden müssen. Daher muss die IT einen Zeitplan aufstellen, der die verschiedenen Phasen realistisch abbildet.

- **Definieren Sie Nutzer und reflektieren Sie die Heterogenität Ihrer Device-Landschaft:** Welchen Mitarbeitern wollen Sie Zugriff zu File-Sharing- und Synchronisationslösungen geben und welche Devices nutzen diese? Ein Unternehmen muss entscheiden, ob es allen Mitarbeitern Zugang zu einer File-Sharing- und Synchronisationslösung gibt oder nur selektiven Gruppen, die zum Beispiel mobil, in virtuellen Teams oder an gemeinsamen Projekten arbeiten. Die Ergebnisse der Umfrage bestätigen, dass Zugangsstrukturen verstärkt nach Projekten, Aufgabenbereichen und Mobilität der Mitarbeiter vergeben werden und weniger auf Hierarchie basierend. Nur 16 % geben ausschließlich Teamleitern und Abteilungsleitern Zugang zu einer File-Sharing- und Synchronisationslösung.
- **Definieren Sie eine Aufgabenstruktur:** Für das kollaborative Arbeiten, aber auch für die Sicherheit der Daten ist es wichtig, klare Tasks zu vergeben. Dokumente oder auch Ordner müssen mit Handlungsvorschriften versehen sein, die dem Nutzer entweder gewisse Aktionen verbieten (zum Beispiel Bearbeiten oder Weiterleiten) oder sie ihm ermöglichen (Speichern oder Drucken eines Dokuments). Dies kann auf Dokumenten-, Ordner- oder auch auf Benutzerebene geschehen.
- **Evaluieren Sie Ihr perfektes Bereitstellungsmodell:** Die Private Cloud ist laut der Umfrage hierzulande das beliebteste Modell (51 %) – allerdings wären auch 26 % der befragten Unternehmen mit einer Public Cloud zufrieden und 32 % ziehen eine hybride Lösung in Erwägung. Obwohl die Datensicherheit bei allen Befragten ein großes Thema ist und auch der Wunsch nach einem Datenzentrum in Deutschland (43 %) dominiert, sind Anwender der Cloud gegenüber offen. Zwar besteht keine bedingungslose Akzeptanz der Cloud – immerhin geben nur 5 % der Befragten an, dass sie diese (egal ob Public oder Private Cloud) für absolut sicher halten, trotzdem ist die Mehrzahl der Befragten bereit, dieses Bereitstellungsmodell für ihre File-Sharing- und Synchronisationslösungen zu nutzen. Anwender sind durch die Datenskandale der letzten Zeit sehr sensibel geworden, was den Missbrauch oder Diebstahl von Daten angeht. Sie sind aber auch geschult genug, um zu erkennen, dass die Cloud durchaus ein guter Weg ist, Daten zentral zu bearbeiten und zu teilen. Wichtig ist die Evaluierung der verschiedenen Modelle: Ob Public oder Private Cloud, On-Premise oder eine hybride Lösung, muss jedes Unternehmen individuell entscheiden.
- **Erweitern Sie ein einheitliches File-Sharing- und Synchronisationstool auf Firmen-Level:** Ein sicheres Teilen, Bearbeiten und Synchronisieren von Dokumenten und Daten kann nur funktionieren, wenn es firmenweit implementiert wird und nicht als selektive Insellösung. Das heißt nicht, dass alle Mitarbeiter Zugriff auf die Daten bekommen müssen, sondern vielmehr soll verhindert werden, dass Mitarbeiter ohne Zugriff sich mit anderen Tools behelfen. Für ein Unternehmen bedeutet das eine Kommunikation auf der gesamten Mitarbeiterebene und auch eine Sensibilisierung derjenigen Mitarbeiter, die keinen Zugriff auf File-Sharing- und Synchronisationslösungen bekommen. Wichtig ist dabei, dass jeder Mitarbeiter die neue Arbeitsweise versteht und sie dementsprechend anwenden kann.
- **Schulen Sie Ihre Mitarbeiter und führen Sie ein Change-Management ein:** Wie die Anwender in der Umfrage bestätigen, war und ist das Versenden von Dokumenten per E-Mail die gängigste Form der Kommunikation

und Kollaboration. Solche etablierten Prozesse können nicht von heute auf morgen umgestellt werden. Unternehmen müssen ihre Mitarbeiter schulen und zügig ein angemessenes Change-Management implementieren, bei dem die Art und Weise, Dokumente auszutauschen, grundlegend verändert wird. Auch die Art der Datenspeicherung ändert sich durch File-Sharing- und Synchronisationslösungen: Die Information befindet sich nicht mehr auf dem eigenen Laptop oder dem Desktop, sondern ist zentral abgelegt.

- **Implementieren Sie Tools zum Monitoring und zur Kontrolle:** Richtlinien sind nur sinnvoll, wenn sie auch eingehalten werden. Daher sind eine Kontrolle und kontinuierliches Monitoring der Mitarbeiter und ihrer Arbeitsweise vonnöten. Damit Dokumente nicht unautorisiert an Dritte gelangen, muss die IT gewisse Warn-Tools implementieren, die hochsensible Daten schützen. Aber auch beim Ausscheiden eines Mitarbeiters aus der Firma oder bei Verlust oder Diebstahl eines mobilen Endgerätes muss die IT sofort handeln können und jeglichen Zugriff der Person oder des Device auf Firmendaten unterbinden.

Methodik

Bei dem vorliegenden Dokument handelt es sich um einen Auszug aus der Multi-Client-Studie „Mobile Content Management in Deutschland 2014“, die von verschiedenen Anbietern gesponsert wurde.

Ziel der im Dezember 2013 durchgeführten Marktbefragung unter 238 Unternehmen in Deutschland mit mindestens 100 Mitarbeitern war es, die aktuellen Trends und Pläne für Maßnahmen zur Implementierung von File-Sharing- und Synchronisationslösungen zu ermitteln. Vor dem Hintergrund des immer größer werdenden Einflusses von Management und Fachabteilungen auf IT-Entscheidungen setzt sich die Stichprobe zur Hälfte je aus IT und Fachbereichsentscheidern zusammen.

Die nachfolgende Fallstudie basiert auf Informationen, die von Acronis zur Verfügung gestellt wurden. Für diese Angaben übernimmt IDC keine Gewähr.

Fallstudie: Zentrale Informatikdienste der Kantonalen Verwaltung Basel-Stadt

WWW.ACRONIS.DE

Informationen zum Kunden

Die Verwaltung des Kantons Basel-Stadt hat sieben unterschiedliche Bereiche, das Präsidialdepartement, Finanzen, Bau- und Verkehr, Erziehung, Gesundheit, Justiz und Sicherheit sowie Wirtschaft, Soziales und Umwelt - mit insgesamt 5000 Mitarbeiten.

Anforderungen des Kunden

Die Verwaltung des Kantons Basel-Stadt im Norden der Schweiz hat dieselbe Herausforderung wie viele andere Behörden und globale Unternehmen: Mitarbeiter bringen zunehmend ihre mobilen Endgeräte mit zur Arbeit („Bring your own device"; BYOD) und nutzen diese, um auf Unternehmensdokumente und -dateien zuzugreifen.
Mobile Mitarbeiter sollen immer und überall Zugang zu Dateien haben, jedoch müssen dabei Sicherheitsrichtlinien und die Versionskontrolle sichergestellt werden.

Die Kernaufgabe der Zentralen Informatikdienste (ZID) besteht darin, auf anforderungsgerechte, zuverlässige und wirtschaftliche Weise die IT-Grundversorgung einer modernen Verwaltung für den Kanton Basel-Stadt sicherzustellen. Darunter fallen alle Informations- und Kommunikationstechnologien, die ihre Mitarbeiterinnen und Mitarbeiter in einer Verwaltungseinheit unabhängig von ihrem konkreten gesetzlichen Auftrag beziehungsweise ihren spezifischen Geschäftsprozessen einsetzen.

Versionskontrolle ist eine weitere Herausforderung für die IT und deren Anwender. Früher führten Mitarbeiter noch Änderungen an Dateien durch, mailten sich die Dokumente danach an ihren eigenen E-Mail-Account. Erst nach dem Ausdrucken eines Dokuments wurde transparent, dass das Dokument bereits veraltet war oder jemand weiter daran gearbeitet hatte. Während eines Meetings stellte sich letztendlich heraus, dass jeder mit einer anderen Dokumentversion gearbeitet hatte.

Darstellung der Lösung

Sicheres Enterprise File Sharing und Datensynchronisierung

Acronis activEcho ist eine Lösung für Enterprise File Sharing und Datensynchronisierung, mit der Unternehmen und IT-Abteilung die Kontrolle über die Daten zurück erhalten. Die vermehrte Nutzung (privater) mobiler Geräte – Stichwort BYOD (Bring Your Own Device) – sowie die verstärkte Verwendung von Lösungen für Privatanwender wie etwa Dropbox, zwingt Unternehmen dazu, neue Lösungen zu finden, um dem Bedarf der Anwender gerecht zu werden. Diese Lösungen müssen außerdem eine Reihe strenger Anforderungen in Bezug auf Compliance, Sicherheit und Standards der Unternehmensführung erfüllen. activEcho adressiert alle wichtigen Anforderungen der IT, des Unternehmens und der Anwender.

Sicherer mobiler Datenzugriff

Acronis mobilEcho ermöglicht es der IT-Abteilung des Unternehmens sicheren Zugriff von Mobilgeräten auf Unternehmensinhalte, die auf Dateiservern, NAS-Systemen und in SharePoint gespeichert sind, bereitzustellen. Mit Acronis mobilEcho können Unternehmen die Produktivität ihrer Mitarbeiter, die mobile Geräte im Einsatz haben, nach Angaben des Anbieter steigern, während die IT-Abteilung gleichzeitig die Kontrolle über Datensicherheit und Compliance behält. Acronis mobilEcho ist eine sichere Lösung für Mobile File Management (MFM), die mobile Geräte zu echten Business-Plattformen macht. Ferner ist mobilEcho eine gute Ergänzung zu Lösungen für Mobile Device Management (MDM).

Projekt Highlights

Gesucht: Eine Lösung für sichere mobile Datenverwaltung, die sich in die bestehende Infrastruktur integrieren lässt

Auf der Suche nach einer geeigneten Lösung für sichere mobile Datenverwaltung, also Mobile File Management (MFM), analysierte das Team der Zentralen Informatikdienste des Kantons Basel-Stadt verschiedene Lösungen. Dabei stellte sich schnell heraus, dass die Integration in die bestehende Infrastruktur der kantonalen Informatik bei den meisten Anbietern nicht möglich war.

Sebastian Heller, Leiter Client Services bei der ZID steuerte das Pilotprogramm, und führte mobilEcho bei ausgewählten Mitarbeitern der kantonalen Verwaltung Basel-Stadt im November 2011 ein. Trotz langer Planungsphasen im Vorfeld, ging letztendlich die Implementierung der Lösung sehr schnell: die Installation der Software und die Integration in die bestehende Infrastruktur dauerte nur wenige Tage. Dies lag vor allem an der Möglichkeit, mobilEcho in die bestehende Infrastruktur einzubinden.

Das Team entschied sich, die Software über ein virtuelles privates Netzwerk zu betreiben. Dadurch mussten keine Firewalls konfiguriert werden. Auf diese Weise ist der Zugriff auf Dateien so einfach wie das Lesen von E-Mails; auch sind Dateisynchronisierung oder Pfadwechsel durch den Anwender dadurch unnötig.

Mehr Effizienz, weniger Papierverbrauch

Sowohl das ZID-Team als auch die Anwender der kantonalen Verwaltung Basel-Stadt waren von den Vorteilen von mobilEcho überzeugt: denn obwohl die Anwender zu jederzeit unmittelbaren Zugriff auf Unternehmensdaten über ihre mobilen Endgeräte hatten, geschah dies nun unter der Kontrolle der IT und innerhalb der internen Sicherheits- und Managementanforderungen.

Auch das bisherige Problem der unterschiedlichen Dokumentenversionen wurde durch die Möglichkeit der Versionskontrolle bei mobilEcho eliminiert und das sparte der kantonalen Verwaltung auch Geld: durch die Nutzung und die einfache Bedienung dieser Funktionalität druckten die Verwaltungsangestellten weit weniger Dokumente aus. Die kantonale Verwaltung konnte dadurch Kosten einsparen und die Mitarbeiter zu einem nachhaltigeren Umgang mit ihren Ressourcen animieren – ein unbedachter Umweltvorteil, der auf große Zustimmung in der Verwaltung stieß.

In Sitzungen benutzt heute fast keiner mehr Papier. Die Mehrheit greift vom iPad auf Dokumente zu, so als ob er an seinem Arbeitsplatz sitzen würde – einfach mobil, jederzeit und überall.

Highlight 1

mobilEcho ist eine Lösung für Mobile File Management (MFM), mit der ein beliebiges Mobilgerät in eine echte Business-Plattform verwandelt werden kann, da Unternehmen damit die erforderliche strenge Sicherheits- und Verwaltungsgranularität erhalten. Acronis mobilEcho bietet Funktionen zur In App -Bearbeitung von Microsoft Office-Dokumenten, -Tabellen und -Präsentationen, ein FIPS 140-2-zertifiziertes Modul zur Verschlüsselung nach Militärstandard sowie Unterstützung für Office365 gehostete SharePoint-Sites.

Highlight 2

activEcho ist die Enterprise-Lösung für File Sharing und Synchronisierung, die einfache Bedienbarkeit und Effektivität für den Endanwender mit nötigen Funktionen wie Kontrolle, Sicherheit, Verwaltbarkeit und Flexibilität für die IT-Administratoren verbindet.

Highlight 3

Die intuitive Benutzeroberfläche (auch in deutscher Sprache) ermöglicht eine einfache Bedienbarkeit und macht kosten-, sowie zeit-intensive Trainings überflüssig.

Hinweis: Acronis activEcho und Acronis mobilEcho sind seit März 2014 Teil der Acronis Access Lösung.

Zitate des Kunden zum Projekt

"Es ging sehr schnell. In nur einer halben Stunde war die Software installiert und innerhalb einiger Tage voll integriert. Wir konnten Acronis mobilEcho in unsere bestehende Infrastruktur einbauen - das machte den Installationsprozess wirklich einfach."

Von: Sebastian Heller, Leiter Client Services bei der ZID

"Für uns ist es sehr wichtig, Daten und deren Zugriffe verwalten zu können und gleichzeitig zu wissen, wer diese gerade herunterlädt. Wir möchten nicht, dass sich Dokumente außerhalb unserer eigenen IT-Umgebung befinden."

Zitate von Acronis zum Projekt

"Die Arbeitswelt von heute hat sich grundlegend verändert und viele Mitarbeiter arbeiten von zu Hause oder von unterwegs aus"

Von: Anders Lofgren, VP of Product Management bei Acronis

"Wenn IT-Entscheider diese Trends in Angriff nehmen, können sie es Anwendern im Unternehmen mithilfe von mobilEcho und activEcho ermöglichen, mit jedem beliebigen Gerät zu arbeiten und durch die Nutzung der neuen und leicht zu bedienenden Acronis Policy Engine gleichzeitig sicheren Zugriff, Austausch und Synchronisierung bieten. Mit diesen neuen Produkten können IT-Entscheider Mitarbeiter noch einfacher dabei unterstützen, produktiv zu bleiben, ohne auf die Sicherheit und Kontrollmöglichkeiten zu verzichten, die das Unternehmen erwartet."

Interview

MIT SANDRA ADELBERGER, DIRECTOR PRODUCT MARKETING, ACRONIS

Anlässlich der Vorstellung der Ergebnisse der Studie „Enterprise Mobility in Deutschland 2013“ sprach IDC mit Sandra Adelberger, Director Product Marketing bei Acronis.

IDC: *Die Arbeitnehmer in Deutschland werden immer mobiler. Endgeräte, Zugriff und Applikationen stellen die Grundvoraussetzungen für mobiles Arbeiten dar. Jedoch stoßen Mitarbeiter beim Content oft an ihre Grenzen – denn Daten und Dateien sind häufig noch nicht mobil. Welche Hürden sind zu überwinden, damit Mitarbeiter in Bezug auf File Sharing und Synchronisation optimal unterstützt werden?*

Sandra Adelberger: Es gibt zwei Anforderungen in Bezug auf File Sharing und Synchronisation, die sich auf den ersten Blick zu widersprechen scheinen: Einerseits möchte der Anwender für sein mobiles Arbeiten seine gewohnte Umgebung und Tools einsetzen. Außerdem möchte er zu jeder Zeit und von überall auf Daten zugreifen, auch von mehreren Endgeräten aus, gegebenenfalls private Endgeräte eingeschlossen. Auf der anderen Seite stehen die Unternehmensinteressen: das Unternehmen muss verhindern, dass Daten unkontrolliert nach außen gelangen. Deshalb ist es entscheidend, dass die Unternehmens-IT die Kontrolle über den Datenfluss und die Zugangsberechtigungen behält. Das schließt private Geräte mit ein, die beruflich genutzt werden. Eine File Sharing- und Synchronisierungslösung sollte die Anforderungen sowohl der Anwender als auch der Unternehmens-IT erfüllen können.

IDC: *Was empfehlen Sie Unternehmen, die Angst davor haben, Firmeninhalte zentral in der Cloud zu speichern? Wie können diese ihre Unsicherheiten in Bezug auf Datensicherheit und Datenschutz überwinden?*

Adelberger: Unternehmen können ihre Unsicherheiten in Bezug auf Datensicherheit und Datenschutz überwinden, indem sie eine eigene Lösung in Bezug auf File Sharing und Synchronisierung auf einem Unternehmensserver implementieren – und damit innerhalb der Unternehmensinfrastruktur. Diese Lösung sollte Zugriffsmöglichkeiten und Berechtigungen bieten, wie in der vorherigen Frage bereits beantwortet wurde. Damit liegen die Daten selbst und alle Aspekte rund um Datensicherheit und Datenschutz wieder in den Händen der IT.

IDC: *Welche Vorgehensweise empfehlen Sie Unternehmen, um deren Dateien und Dokumente mobil zu machen?*

SANDRA ADELBERGER

Adelberger: Folgende fünf Tipps gibt Acronis für den sicheren mobilen Datenzugriff und mobile Zusammenarbeit:

1. Stellen Sie eine Sicherheitsrichtlinie für mobile Geräte auf! Verpflichten Sie beispielsweise Ihre Anwender, ihre Geräte mit Kennwörtern zu schützen.
2. Hören Sie auf, Ausnahmen von Ihren Regeln zu gestatten! Oftmals gibt es für Mitarbeiter, die auf sensible Daten im Unternehmen zugreifen, Ausnahmen von der BYOD-Richtlinie.
3. Machen Sie alle Mitarbeiter für „sicheres BYOD“ mitverantwortlich und bieten Sie Trainingsmöglichkeiten an, um Mitarbeitern die Risiken von BYOD für die Datensicherheit zu erklären.
4. Bereiten Sie sich auf die Apple-Welle vor! Begegnen Sie der steigenden Anzahl von Apple-Geräten in Ihrem Unternehmen mit Lösungen, um sie problemlos in bestehende Windows-IT-Umgebungen zu integrieren.
5. Unterschätzen Sie nicht die Gefahren öffentlicher Clouds! Öffentliche Clouds bieten einen praktischen Zugriff, sind aber unter anderem nicht sicher. Stellen Sie daher eine Richtlinie zum File Sharing in öffentlichen Clouds auf.

Copyright Hinweis

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte:
Katja Schmalen, Marketing Director, +49 69 90502-115 oder kschmalen@idc.com.

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht ihren Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Durch das Netzwerk der mehr als 1000 Analysten in 110 Ländern mit globaler, regionaler und lokaler Expertise kann IDC ihren Kunden umfassenden Research zu den verschiedensten Segmenten des IT-, TK- und Consumer Marktes zur Verfügung stellen. Seit 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC.

IDC Central Europe GmbH
Hanauer Landstr. 135-137
60314 Frankfurt • Germany

T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com

IDC
Analyze the Future