Xerox® Digital Alternatives
Software-Benutzerhandbuch zur Sicherheit und Evaluierung

Oktober 2016
Version 2.0.xx

Dieses Dokument wird regelmäßig überarbeitet. Änderungen, technische Ungenauigkeiten sowie orthografische und typografische Fehler werden in der jeweils nachfolgenden Ausgabe berichtigt.

Änderungsübersicht

Datum	Versionsnummer	Beschreibung
October 2016	2.0.xx	• Nach Versionsfreigabe vorgenommene Aktualisierung zur Verschlüsselung der E-Mail-Adressen
Januar 2016	2.0	• Schließt Text zu den neuen Funktionen in Digital Alternatives 2.0 ein
Mai 2015	1.2	• Schließt Möglichkeit zur Bereitstellung von Digital Alternatives 1.2 in der Private Cloud ein
März 2015	1.1	• Großangelegte Umstrukturierung, um Übereinstimmung mit der Vorlage für interne Sicherheitsdokumentation herzustellen • Aktualisierungen für Version 1.1, einschließlich Einführung in die Nutzung in Cloud
August 2014	1.0	Erstfassung

Inhaltsverzeichnis

Abbildungen

1 Einführung

Produktüberblick

Xerox® Digital Alternatives ist eine Software, mit der Sie Dokumente digital lesen, kommentieren und gemeinsam nutzen können. Sobald ein Dokument in den DA-Client des Benutzers importiert wird, werden automatisch Kopien dieses Dokuments auf allen Geräten (PC und iPad) des Benutzers erstellt, auf denen der DA-Client installiert wurde. Zudem können kommentierte Dokumente mithilfe der Anwendung oder per E-Mail gemeinsam mit anderen Benutzern genutzt werden.

Xerox® Digital Alternatives besteht aus fünf Hauptkomponenten.

Komponente	Beschreibung
Lokaler Server von Xerox® Digital Alternatives	• Führt alle Schritte der Authentifizierung durch • Erstellt Kopien von Dokumenten auf den eigenen Geräten und den Geräten anderer Benutzer
Endbenutzer-Client-Softwareanwendung	• Wird auf dem Windows®-PC, iPad®, unterstützten Android™ - Tablets oder dem Apple Macintosh®-Computer des Endbenutzers installiert • Ermöglicht das Kommentieren und die Überarbeitung von Dokumenten
Xerox® CompleteView® Data Communicator zur Berichterstellung	• Sendet Nutzungsdaten vom lokalen Server von Digital Alternatives an die CompleteView®-Berichtsplattform von Digital Alternatives, die innerhalb von Xerox gehostet wird
CompleteView-Berichterstellung für Digital Alternatives	• Erstellt für Kunden mithilfe von Nutzungsdaten aus dem lokalen Server von Xerox® Digital Alternatives und auf Grundlage branchenüblicher Metriken eine Analyse der Nutzungsvorteile Wird im Netzwerk von Xerox gehostet
Internetbasierter Zentralserver von Digital Alternatives	• Speichert die vom lokalen Server und den Clients verwendeten Konto- und Lizenzierungsdaten

Lokaler Server von Xerox® Digital Alternatives – Arten der Bereitstellung

Implementierung vor Ort

Bei der Implementierung vor Ort werden für den Benutzer von Xerox® Digital Alternatives alle Schritte zur Authentifizierung mit dem Active Directory® der IT-Abteilung des Kunden durchgeführt. Der Benutzer gibt über die Endbenutzer-Client-Anwendung von Xerox® Digital Alternatives die Zugangsdaten ein. Darüber hinaus lassen sich mithilfe des lokalen Servers von Xerox® Digital Alternatives Kopien von Dokumenten auf allen Geräten erstellen, für die die jeweiligen Dokumente freigegeben werden. Werden Dokumente gemeinsam mit anderen Benutzern von Xerox® Digital Alternatives genutzt, kann für die Endbenutzer-Client-Anwendung mit dem lokalen Server von Xerox® Digital Alternatives eine globale Adresssuche durchgeführt werden. Wenn ein Dokument gemeinsam mit einem Anwender genutzt wird, der Digital Alternatives nicht verwendet, dann sendet der lokale Server von Xerox® Digital

Alternatives das Dokument über den E-Mail-Server des Kunden an die Endbenutzer-Client-Anwendung. Die Interaktion zwischen dem lokalen Server von Xerox® Digital Alternatives und dem Internet-basierten Zentralserver dient dazu, Benutzern außerhalb der Netzwerkinfrastruktur des Kunden auf Wunsch Dokumente zur Verfügung stellen zu können.

Implementierung in Private Cloud

Xerox bietet die Möglichkeit, den lokalen Server für den Digital Alternatives-Kunden im Netzwerk der Private Cloud von Xerox® zu hosten. In diesen Fällen ist keine Installation von Server-Software am Standort des Kunden erforderlich. Zudem muss der Kunde den physischen Server nicht länger verwalten, da dies von Xerox übernommen wird. Zur Bereitstellung in der Private Cloud ist eine spezielle VPN-Verbindung zwischen dem Netzwerk des Kunden und der Netzwerkumgebung der Private Cloud von Xerox® erforderlich. Über die sichere VPN-Verbindung zwischen den beiden Netzwerken muss zudem vom Anwendungsserver in der Private Cloud auf Active Directory und LDAP-Ressourcen des Kunden zugegriffen werden können. Alle Funktionen des lokalen Servers, die auch bei der Implementierung des lokalen Servers vor Ort gegeben sind, werden bei Implementierung in der Private Cloud ebenfalls unterstützt.

Zur Verwendung dieses Handbuchs

Dieses Handbuch soll den zuständigen Mitarbeitern von Xerox und Partnern dabei helfen, der IT-Abteilung eines potentiellen Kunden Informationen zur Sicherheit von Digital Alternatives an die Hand zu geben und ihm bei der Zertifizierung der Bereitstellung von Xerox® Digital Alternatives in seiner IT-Umgebung zur Seite zu stehen. Mitarbeiter des Kunden sowie Mitarbeiter von Xerox können dieses Handbuch im Rahmen der Evaluierungen vor dem Verkauf, der Prüfungen im Anschluss an den Verkauf und des Abnahmeverfahrens verwenden. Die eigentlichen Prüfpläne und Abnahmekriterien hängen von den Formalitäten bzw. der Dokumentation des jeweiligen Kunden ab. Dieses Handbuch enthält Informationen zu potentiellen Auswirkungen von Xerox® Digital Alternatives auf die Sicherheit, die IT-Infrastruktur von Unternehmen, den Netzwerkverkehr, die Ressourcen und die Planungserfordernisse.

Dieses Handbuch ist in erster Linie zur Verwendung während der Implementierung und nach der Vertragsunterzeichnung gedacht. In Verbindung mit einer Geheimhaltungsvereinbarung kann es auch zur Verkaufsvorbereitung und bei der Durchführung von Evaluierungen eingesetzt werden.

Zielpublikum

Dieses Handbuch richtet sich an die IT-, Sicherheits- und Management-Organisationen sowie die Unternehmensführung von Kunden. Vor der Zertifizierung von Xerox® Digital Alternatives sollten sich Kunden und die zuständigen Mitarbeiter von Xerox vertraut machen mit:

- der IT-Umgebung am Standort, an dem Xerox® Digital Alternatives installiert wird
  - Wird die Option zum Hosting des lokalen Servers in der Private Cloud genutzt, sind Kenntnisse über VPN-Verbindungen und der dazugehörigen Sicherheitsaspekte erforderlich.
- allen Einschränkungen, die für in diesem Netzwerk verwendete Anwendungen gelten
- dem Betriebssystem Microsoft® Windows Server®
- dem Datenbanksystem Microsoft SQL Server®

Geltungsbereich dieses Handbuchs

Xerox® Digital Alternatives lässt sich nach Wunsch konfigurieren und bietet eine Vielzahl von Funktionen. In diesem Handbuch werden Standardimplementierungen und die IT-Umgebung eines typischen Kunden beschrieben. Wenn die IT-Umgebung des Kunden von der hier beschriebenen Umgebung abweicht, muss das IT-Team des Kunden gemeinsam mit dem zuständigen Mitarbeiter von Xerox die Unterschiede ausfindig machen und alle potentiellen Problembereiche beseitigen.

Die in diesem Handbuch enthaltenen Informationen beziehen sich auf Version 2.0 von Xerox® Digital Alternatives. Obwohl diese Informationen im Großen und Ganzen unverändert bleiben, beziehen sich manche Angaben nur auf eine bestimmte Version und müssen daher regelmäßig aktualisiert werden. IT-Abteilungen sollten sich bei Ihrem jeweiligen Ansprechpartner bei Xerox nach der jeweils aktuellen Fassung erkundigen.

Neuerungen in Version 2.0

Digital Alternatives Version 2.0 bietet eine Reihe neuer Möglichkeiten.

- Verschiedene integrierte Dokumenten-Workflows ermöglichen Kunden die Beteiligung verschiedener Benutzer von Digital Alternatives an gängigen Workflow-Aufgaben wie Überarbeitung, Genehmigung und Unterzeichnung von Dokumenten.

- Die Integration mit dem E-Signatur-Dienst DocuSign® ermöglicht Benutzern die Übermittlung von Dokumenten zur Unterzeichnung. So können sie über ihr vorhandenes DocuSign-Konto rechtsgültige digitale Unterschriften anfordern.

- Digital Alternatives bietet nun auch direkte Integration mit der Content-Management-Plattform Xerox® DocuShare®. Dies ermöglicht den Import und Export von Dokumenten in und aus DocuShare.

- Außerdem wird die Client-Software von Digital Alternatives nun auf zwei neuen Hostplattformen, nämlich Google Android-Tablets und Apple Macintosh-Computern, unterstützt.

Dokumentenverarbeitungs-Workflows von Digital Alternatives

Digital Alternatives bietet integrierte Verwaltung von Dokumenten-Workflows. Benutzer können Dokumente innerhalb von Digital Alternatives zur Prüfung, Unterzeichnung oder Genehmigung an andere Benutzer senden. Bei jeder Workflow-Funktion wird der Empfänger über den Eingang einer neuen Workflow-Anforderung benachrichtigt. Wenn der beauftragte Empfänger die Aufgabe abgeschlossen hat, wird das bearbeitete Dokument automatisch mit Bearbeitungsdatum und eventuellen Kommentaren des Bearbeiters an den Absender zurückgesendet.

Workflow-Anforderungen können auch an Empfänger außerhalb des Digital Alternatives-Systems gesendet werden. In diesem Fall wird das Dokument als E-Mail-Anlage übermittelt, wird jedoch nach Bearbeitung nicht an den Absender in Digital Alternatives zurückgesendet.

Integration mit dem E-Signatur-Dienst DocuSign®

Bei Kunden, die ein DocuSign-Unternehmenskonto für elektronische Unterschriften haben, können Benutzer von Digital Alternatives Dokumente über ihr eigenes DocuSign-Konto zur Unterzeichnung an einen Empfänger senden. Das Dokument wird automatisch in das DocuSign-Konto des Absenders hochgeladen, und der Empfänger wird per E-Mail von DocuSign davon benachrichtigt, dass eine Unterzeichnungsanforderung eingegangen ist. Nach erfolgreichem Hochladen des Dokuments in DocuSign werden alle weiteren Schritte zur Bearbeitung der Unterzeichnungsanforderung in DocuSign ausgeführt. Nachdem der Empfänger die Unterzeichnungsanforderung bearbeitet hat, wird das unterzeichnete Dokument nicht automatisch an das Konto des Benutzers bei Digital Alternatives zurückgesendet, sondern verbleibt in DocuSign.

Integration mit dem Content-Management-System Xerox® DocuShare®

In Digital Alternatives können Dokumente aus der Client-Anwendung heraus in ein entsprechend konfiguriertes DocuShare-System hochgeladen und daraus heruntergeladen werden. Zum Zugriff auf DocuShare benötigt der Benutzer ein eigenes Benutzerkonto für DocuShare, das unabhängig von dem Konto ist, über das sich der Benutzer bei Digital Alternatives anmeldet. Damit der Direktzugriff funktioniert, muss die Client-Anwendung von Digital Alternatives außerdem direkten Netzwerk-Zugriff auf den DocuShare-Server haben. Die Nutzung dieser Funktion ist daher für Benutzer außerhalb eines Unternehmensnetzwerks u. U. nicht möglich, sofern ihre Client-Geräte nicht über eine VPN-Verbindung zum Unternehmensnetzwerk verfügen.

Neue Host-Plattformen für die Client-Anwendung – Google Android und Apple Macintosh

Die Client-Anwendung von Digital Alternatives unterstützt neben aktuellen Windows-PCs und Apple® iPad-Tablets auch Macintosh-Computer und bestimmte Google Android-Tablets. Weitere Informationen darüber, welche Geräte von der Client-Anwendung von Digital Alternatives unterstützt werden, sind im Systemhandbuch zu Xerox® Digital Alternatives zu finden.

Software-Lizenzierung

Die Software-Lizenzierung wird auf der Kontoebene verwaltet, die in dem im Zentralserver von Digital Alternatives festgelegten Kundenkonto gespeichert wurde. Für die Client-Anwendung des Endbenutzers und den lokalen Server liegen keine eigenen Lizenzen vor. Vielmehr verringert sich die im Zentralserver verwaltete Anzahl der insgesamt verfügbaren Lizenzen, wenn sich ein neuer Endbenutzer zum ersten Mal in seinem Konto in Digital Alternatives anmeldet. Die erste Anmeldung eines Kunden nennt sich Onboarding (Registrierung). Wenn Sie die Endbenutzer-Client-Software deinstallieren, wird dadurch die ursprüngliche Anzahl an verfügbaren Lizenzen nicht wiederhergestellt. Wenn alle auf dem Zentralserver verfügbaren Lizenzen an registrierte Kunden vergeben wurden, müssen von Xerox zusätzliche Lizenzen erworben werden.

Benutzerlizenzen können von einem Benutzer an einen anderen weitergegeben werden, indem das Konto eines Benutzers auf dem lokalen Server deaktiviert wird, sodass dieser Benutzer nicht mehr mit Digital Alternatives arbeiten kann. Nachdem ein Benutzerkonto deaktiviert wurde, wird die betreffende Lizenz wieder frei und kann einem anderen Benutzer innerhalb des Kundenkontos zugewiesen werden.

Regelkonformität und Zertifizierung der Anwendung

Implementierung – IT-Abteilung des Kunden

Die Zertifizierung und Genehmigung der Bereitstellung und des Betriebs von Xerox® Digital Alternatives innerhalb der Netzwerkumgebung erfolgt durch die IT-Abteilung des jeweiligen Kunden. Manche Kunden nutzen ggf. ein inoffizielles Zertifizierungsverfahren, das sich auf die Durchsicht der Dokumentation von Xerox® Digital Alternatives und eine Präsentation von Xerox beschränkt. Der Kunde kann aber auch ein offizielleres Verfahren nutzen, das die Installation und Prüfung mit festgelegten Prüfkriterien und einem festgelegten Prüfplan erforderlich macht. Der Kunde muss die Zertifizierungskriterien bestimmen und zusammen mit dem zuständigen Team von Xerox die erforderlichen Schritte und den Zeitplan festlegen.

Benutzerdaten, die auf den lokalen Servern gespeichert sind, welche im Netzwerk des Kunden implementiert sind, werden nicht auf Server außerhalb des Kundennetzwerks übertragen – eine Ausnahme bilden die Nutzungsdaten, die regelmäßig an die Berichtsserver von Xerox exportiert werden. Dabei handelt es sich um eine optionale Komponente der Lösung, und es werden nur die benutzerbezogenen Daten übermittelt, die unter Tabelle 1: In Digital Alternatives gespeicherte Benutzerdaten aufgeführt sind.

Implementierung – Private Cloud

Xerox ist verantwortlich für die Zertifizierung und Abnahme der Bereitstellung von Xerox® Digital Alternatives in der Private Cloud-Umgebung für einen gegebenen Private Cloud-Kunden. Auf Anforderung kann Xerox die Verfahrensweise für die Zertifizierung und Abnahme der Implementierung dem Kunden zur Verfügung stellen.

Benutzerdaten, die auf den lokalen Servern gespeichert sind, welche im Netzwerk der Private Cloud implementiert sind, werden nicht auf Server außerhalb dieses Cloud-Netzwerks übertragen – eine Ausnahme bilden die Nutzungsdaten, die regelmäßig an die Berichtsserver von Xerox® exportiert werden. Dabei handelt es sich um eine optionale Komponente der Lösung, und es werden nur die benutzerbezogenen Daten übermittelt, die unter Tabelle 1: In Digital Alternatives gespeicherte Benutzerdaten aufgeführt sind.

Die Server von Kunden in Europa, die die Implementierung in der Private Cloud wählen, werden ihren Standort in einer der beiden europäischen Hosting-Rechenzentren haben, die unter Tabelle 2: Hosting-Standorte der Private Cloud aufgeführt sind.

Implementierung – Autorisierte Xerox®-Dienstanbieter für Digital Alternatives

Mitarbeiter von autorisierten Xerox®-Dienstanbietern für Digital Alternatives können am Zertifizierungsprozess beteiligt sein und helfen, zu bestimmen, welche Funktionen und Merkmale von Xerox® Digital Alternatives benötigt werden und wie häufig Aktivitäten im Zusammenhang mit Xerox® Digital Alternatives stattfinden sollen.

Laufende Aufgaben und Zuständigkeiten

Im Rahmen des Zertifizierungsverfahrens müssen die für Kundenkonten zuständigen Mitarbeiter von Xerox in Zusammenarbeit mit dem im Außendienst tätigen Analytiker, der an der Bereitstellung und laufenden Wartung beteiligt ist, und der IT-Abteilung des Kunden die Aufgaben und Zuständigkeiten für die laufende Betreuung der Installation von Xerox® Digital Alternatives festlegen:

- Zuständigkeit des Systemadministrators
  - Die Unterstützung der Server-Hardware ist die Aufgabe der IT-Managementorganisation des Kunden. Für die periodische Installation von Aktualisierungen des Microsoft®-Betriebssystems ist die IT-Abteilung des Kunden zuständig.
- Zuständigkeit für die Backup-Sicherung der lokalen Server-Datenbank und des Dokumentenarchivs
  - Die IT-Abteilung des Kunden ist für die Erstellung von Backups der SQL Server® Datenbank zuständig, die von Xerox® Digital Alternatives genutzt wird. Die IT Abteilung des Kunden ist auch für die regelmäßige Backup-Sicherung des Dokumentenarchivs zuständig.
- Zuständigkeit für die Überwachung des Zustands der lokalen Server-Hardware
  - Die IT-Abteilung des Kunden ist für die Überwachung der Hardware und des Betriebssystems der lokalen Server zuständig. Zum Zuständigkeitsbereich gehören Hardware-Fehler, Fragen der Speicherkapazität auf den Festplatten, der Netzwerkverbindungen und des Betriebssystems.
- Software-Aktualisierungen für lokale Server
  - Der autorisierte Xerox®-Dienstanbieter für Digital Alternatives ist dafür zuständig, zusammen mit der IT-Abteilung des Kunden Upgrades der Software für lokale Server zu planen und durchzuführen, sobald diese verfügbar werden.

2 Architektur

Xerox® Digital Alternatives besteht aus fünf Hauptkomponentenbereichen.

Komponente	Beschreibung
Lokaler Server von Xerox® Digital Alternatives	• führt alle Schritte der Authentifizierung durch • erstellt Kopien von Dokumenten auf den eigenen Geräten und den Geräten anderer Benutzer
Endbenutzer-Client-Softwareanwendung	• wird auf dem Windows®-PC, iPad®, unterstützten Android™-Tablets oder dem Apple Macintosh®-Computer des Endbenutzers installiert • ermöglicht das Kommentieren und die Überarbeitung von Dokumenten
CompleteView® Data Communicator zur Berichterstellung	• sendet Nutzungsdaten vom lokalen Server von Digital Alternatives an die CompleteView®-Berichtsplattform von Digital Alternatives, die innerhalb von Xerox gehostet wird
CompleteView-Berichterstellung für Digital Alternatives	• erstellt für Kunden mithilfe von Nutzungsdaten aus dem lokalen Server von Xerox® Digital Alternatives und auf Grundlage branchenüblicher Metriken eine Analyse der Nutzungsvorteile Wird im Netzwerk von Xerox gehostet
Internet-basierter Zentralserver von Digital Alternatives	• speichert die vom lokalen Server und den Clients verwendeten Konto- und Lizenzierungsdaten

Systemkomponenten

Xerox® Digital Alternatives – Endbenutzer-Client-Anwendung

Diese Software, die auf dem PC, iPad, Android Tablet oder Apple Macintosh-Computer des Endbenutzers installiert werden kann, zeigt Dokumente an und speichert lokale Kopien davon im lokalen Dokumentenarchiv von Digital Alternatives. Die Benutzer haben über die Client-Anwendung Zugriff auf ihre Dokumente. Auf die lokalen Dokumente kann ohne die Client-Anwendung von Digital Alternatives nicht direkt zugegriffen werden. Alle in Digital Alternatives gespeicherten Dokumente werden in in PDF-Dateien konvertiert. Dokumente, die in der Client-Anwendung gespeichert werden, werden automatisch mit dem Konto des Benutzers auf dem lokalen Server synchronisiert. Der Benutzer sieht die Dokumente, die in seinem Konto gespeichert sind, sowie diejenigen, die andere Benutzer für ihn freigegeben haben.

Xerox® Digital Alternatives – Lokale Server-Anwendung

Die lokale Server-Anwendung, die von einem autorisierten Xerox®-Dienstanbieter für Digital Alternatives installiert wird, muss Zugriff auf eine SQL Server®-Datenbank und den Webserver mit Windows Internet Information Services haben. Der lokale Server koordiniert den Dokumentenaustausch zwischen den Geräten eines Benutzers oder mit anderen Benutzern bei Freigabeanforderungen. Jede Client-Anwendung von Digital Alternatives kommuniziert bei der Benutzerauthentifizierung und bei Import oder Änderung eines Dokuments mit der lokalen Server-Anwendung. Das Hosting der Anwendungsserver auf separaten virtuellen Maschinen wird unterstützt.

Da Benutzerkonten über das Active Directory des Kunden eingerichtet und authentifiziert werden, werden die Anmeldedaten, mit der sich ein Benutzer bei der Client-Software anmeldet, zur Authentifizierung anhand des Active Directorys des Kunden an den lokalen Server übermittelt. Diese Kommunikation zwischen lokalem Server und Active Directory des Kunden erfolgt über LDAP (Lightweight Directory Access Protocol).

Berichterstellungs-Anwendung Data Communicator

Die Software-Komponente Data Communicator zur Berichterstellung, die separat auf dem lokalen Server von Xerox® Digital Alternatives installiert wird, extrahiert die Nutzungsdaten des Kunden aus der Berichtsdatenbank auf dem lokalen Server und sendet sie an die CompleteView-Benutzeranalyse-Server für Digital Alternatives, die innerhalb von Xerox gehostet werden. Anhand dieser Daten werden von den CompleteView-Berichtsservern Nutzungsanalyseberichte erstellt. Data Communicator wird so konfiguriert, dass keine personenbezogenen Daten (PII – Personally Identifiable Information) an die CompleteView-Server für Digital Alternatives übertragen werden. Das Systemhandbuch zu Digital Alternatives enthält Informationen über die Konfiguration von Reporting Data Communicator zur Übermittlung von Berichtsdaten an die CompleteView-Benutzeranalyse-Server für Digital Alternatives. Zugriff auf alle Berichte für Digital Alternatives erfolgt über den von Xerox gehosteten CompleteView-Berichtsserver. Berichte können nicht direkt von den lokalen Servern von Digital Alternatives abgerufen werden.

Data Communicator kann so konfiguriert werden, dass personenbezogene Daten (PII) vom Hochladen in den CompleteView-Berichterstattungsserver ausgeschlossen werden. Data Communicator kann bei der Implementierung auf dem Server so konfiguriert werden, dass bestimmte als PII geltende Datenelemente verschleiert werden. Die Tabelle unten zeigt, welche Datenelemente gesendet werden und welche verschleiert werden, wenn keine PII-Daten für den Berichterstattungsserver für Xerox® Digital Alternatives weitergegeben werden sollen.

Datenelement	Digital Alternatives	Digital Alternatives ohne PII
UserID (Benutzer-ID)	Im Klartext übermittelt	Im Klartext übermittelt
Username (Benutzername)	Im Klartext übermittelt	Verschleiert
E-Mail	Im Klartext übermittelt	Verschleiert
Documents (Dokumente)	Im Klartext übermittelt	Im Klartext übermittelt
StorageUsed (Belegter Speicher)	Im Klartext übermittelt	Im Klartext übermittelt
Quota (Kontingente)	Im Klartext übermittelt	Im Klartext übermittelt
DeviceID (Geräte-ID)	Im Klartext übermittelt	Im Klartext übermittelt
ClientTypeID (Kundentyp-ID)	Im Klartext übermittelt	Im Klartext übermittelt
Type (Typ)	Im Klartext übermittelt	Im Klartext übermittelt
ActivityTypeID (Aktivitätstyp-ID)	Im Klartext übermittelt	Im Klartext übermittelt
ActivitySubTypeID (Aktivitäts Untertyp-ID)	Im Klartext übermittelt	Im Klartext übermittelt
ActivityID (Aktivitäts-ID)	Im Klartext übermittelt	Im Klartext übermittelt
Key (Schlüssel)	Im Klartext übermittelt	Im Klartext übermittelt
Value (Wert)	Im Klartext übermittelt	Im Klartext übermittelt
DocumentName (Dokumentname)	Im Klartext übermittelt	Verschleiert

Datenelement	Digital Alternatives	Digital Alternatives ohne PII
Pages (Seiten)	Im Klartext übermittelt	Im Klartext übermittelt
IsColor (Farbe?)	Im Klartext übermittelt	Im Klartext übermittelt
DateUTC (Datum/UTC)	Im Klartext übermittelt	Im Klartext übermittelt
Description (Beschreibung)	Im Klartext übermittelt	Im Klartext übermittelt
ActivityKeyValuePairID (Aktivitätenschlüssel-Wertepaar-ID)	Im Klartext übermittelt	Im Klartext übermittelt
OnboardDateUTC (Registrierungsdatum/UTC)	Im Klartext übermittelt	Im Klartext übermittelt
RecType (Datensatztyp)	Im Klartext übermittelt	Im Klartext übermittelt

Tabelle 1: In Digital Alternatives gespeicherte Benutzerdaten

Die Server werden im Hosting-Rechenzentrum für die Private Cloud von Xerox® gehostet. Die Kommunikation mit diesen Servern von Data Communicator aus erfolgt über das sichere HTTPS-Protokoll und Port 443. Die CompleteView-Server bieten eine sichere Web-Bedienungsoberfläche, über die autorisierte Benutzer auf die Berichtsfunktion von CompleteView zugreifen können. Benutzer können nur Daten aus denjenigen Konten bei Digital Alternatives sehen, für die sie Leseberechtigung haben. Konten von Data Communicator können Daten nur an ein bestimmtes CompleteView-Konto senden, für das sie konfiguriert sind.

Zentralserver von Xerox® Digital Alternatives

Der Zentralserver von Digital Alternatives wird im für Xerox bestimmten Netzwerk der Microsoft Azure-Cloud gehostet. Nur Anwendungssupport-Mitarbeiter für Xerox® MPS, die für die Erstellung und Pflege von Kundenkonten auf dem Zentralserver zuständig sind, haben Zugriff auf den Zentralserver von Digital Alternatives. Die gesamte Kommunikation vom lokalen Server und von der Client-Software an den Zentralserver erfolgt über das sichere HTTPS-Protokoll.

Diese Komponente enthält die vom lokalen Server und den Clients verwendeten Konto- und Lizenzierungsdaten. Der Zentralserver verwaltet das Kundenkonto bei Digital Alternatives, das die für jede Kundenimplementierung von Digital Alternatives vom Zentralserver generierte Kunden-ID sowie die damit verbundenen Kunden-E-Mail-Domäne(n) enthält, über die Benutzer auf ihr Konto bei Digital Alternatives zugreifen. Die im Zentralserver gespeicherten Benutzerdaten schließen nur die E-Mail-Adressen derjenigen Benutzer ein, die die Client-Software installiert und sich bereits einmal bei Digital Alternatives angemeldet haben. Diese E-Mail-Adressen sind verschlüsselt. Auf dem Zentralserver werden keine weiteren Benutzerdaten gespeichert.

In diesem Kundenkonto von Digital Alternatives werden die Lizenzierungskontigente für jede Implementierung verwaltet. Weitere Informationen zur Lizenzverwaltung siehe Systemhandbuch zu Xerox® Digital Alternatives.

Die Diagramme unten zeigen die beiden Bereitstellungsszenarios für die lokalen Serverkomponenten von Digital Alternatives. Bei Implementierung am Standort wird der lokale Server von Digital Alternatives in der IT-Umgebung des Kunden implementiert. Der Kunde stellt die Windows-Server einschließlich des Microsoft SQL-Servers bereit. Bei Implementierung in der Private Cloud stellt Xerox die Hosts und die SQL-Server im Netzwerk seiner Private Cloud sowie eine VPN-Verbindung zwischen dem Netzwerk der Xerox® Private Cloud und dem IT-Netzwerk des Kunden bereit.

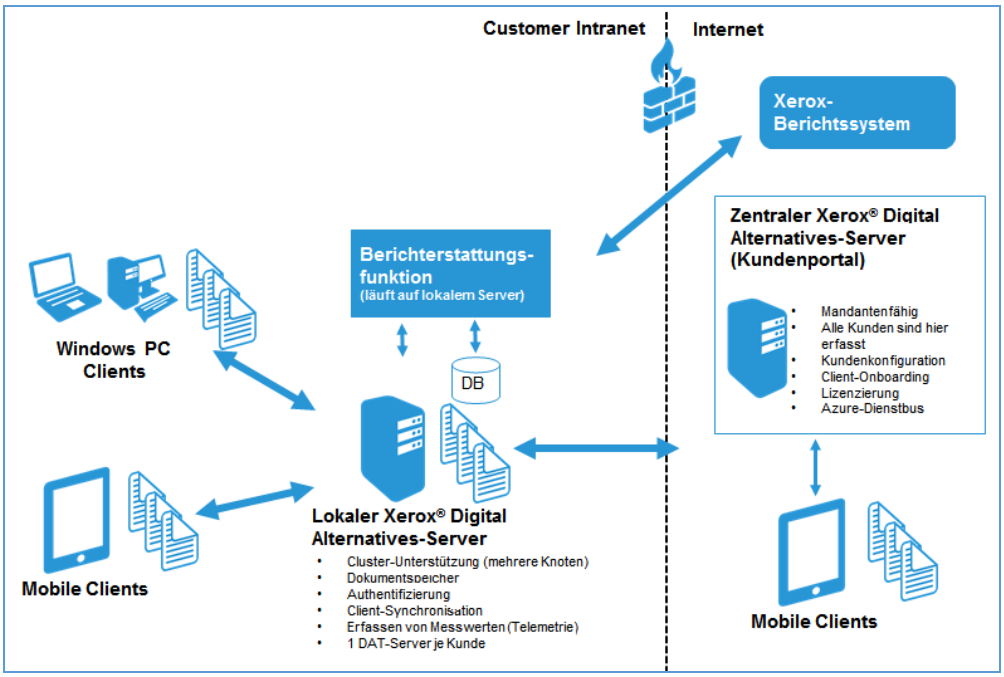

Abbildung 1: Implementierung vor Ort

Bei der Implementierung in der Private Cloud richten wir eine spezielle Business-to-Business-VPN-Verbindung zwischen dem Anwendungsserver im Netzwerk von Xerox Services und der Netzwerkumgebung des Kunden ein, die dem Anwendungsserver Zugriff auf das Active Directory und die Exchange-LDAP-Verbindungen des Kunden verschafft. Die VPN-Verbindung ermöglicht auch Benutzern mit der Client-Benutzersoftware von Digital Alternatives die Herstellung einer Verbindung zum Anwendungsserver aus der Netzwerkumgebung des Kunden heraus.

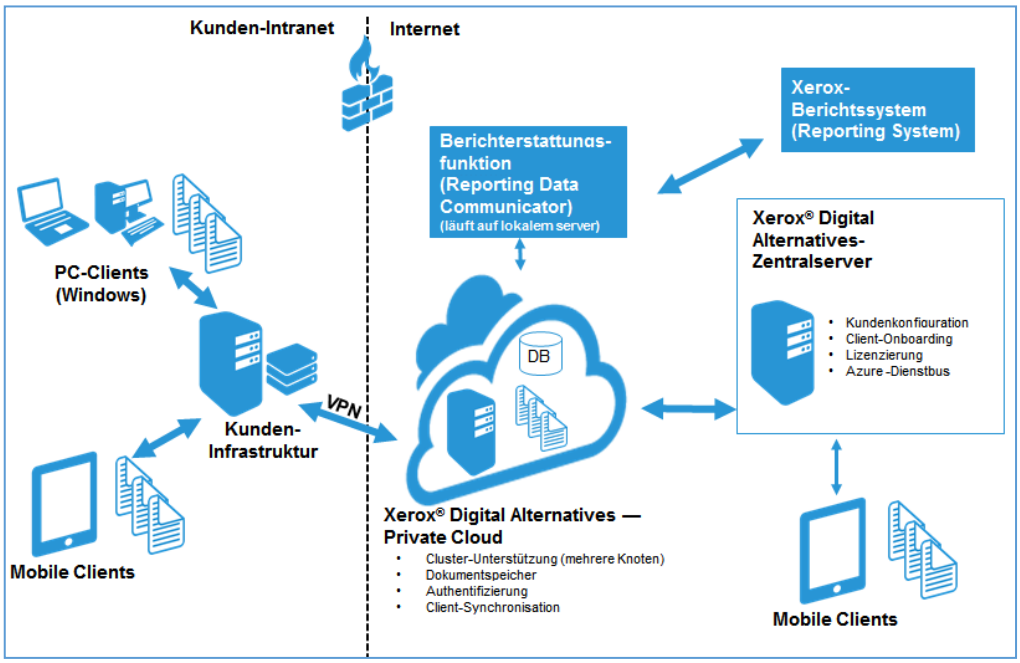

Abbildung 2: Implementierung in Private Cloud

Modelle der Bereitstellung des lokalen Servers

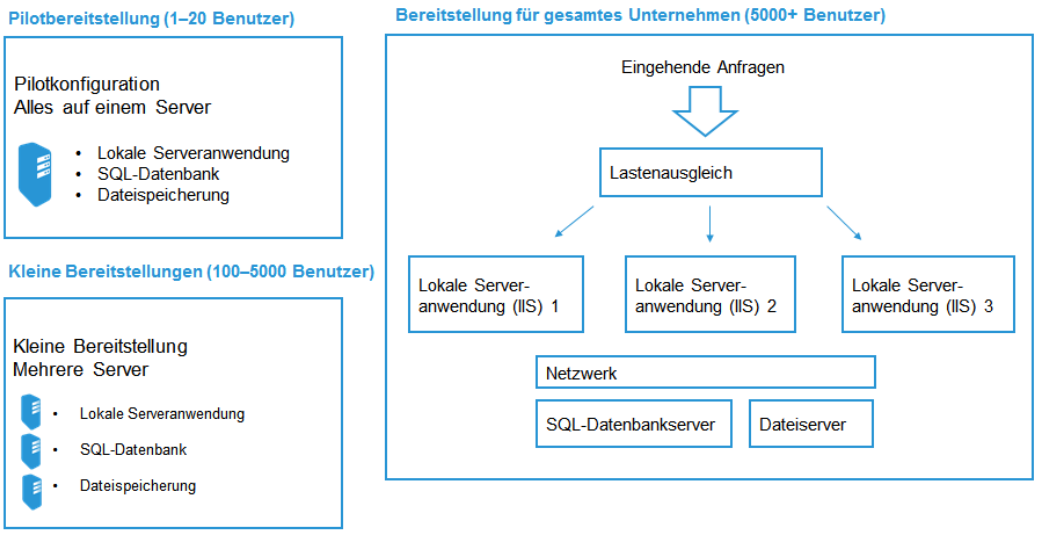

Abbildung 3: Modell der Bereitstellung des lokalen Servers

3 Lösung / Anwendungs-umgebungen

Hardware- und Software-Anforderungen

In den folgenden Abschnitten finden Sie detaillierte Informationen zu den Hardware- und Softwareanforderungen für den lokalen Server und die Client-Software von Digital Alternatives. Die meisten Angaben beziehen sich auf den lokalen Server, aber Sie finden darin auch Informationen zu PC und iPad.

Lokaler Server – Installationsvoraussetzungen

Unterstützte Betriebssysteme

- Windows® 2008 Standard
- Windows® 2008 Enterprise
- Windows® 2008 R2 Standard
- Windows® 2008 R2 Enterprise
- Windows® 2012
- Windows® 2012 R2

Sonstige erforderliche Software

- Microsoft® .NET Framework 4.5.2
- Windows-Aufgabenplanung
- Microsoft Message Queuing (MSMQ)

Hardwarevoraussetzungen

- RAM: 8 GB
- CPU: Dual Core 1,20 GHz
- Festplatte: 260 GB

Für die Installation der Software sind mindestens 100 MB freier Speicherplatz erforderlich. Dies schließt den Speicherplatz für das Dokumentenarchiv nicht ein. Der Anwendungsserver (Webserver) erfordert, dass das Serverzertifikat auf den IIS-Webserver des Servers angewendet wird, damit verschlüsselte Kommunikation mit Client-Anwendungen über das HTTPS-Protokoll mit SSL (Secure Sockets Layer) möglich ist. Die gesamte Kommunikation zwischen den Anwendungskomponenten von Digital Alternatives erfolgt über das HTTPS-Protokoll.

Data Communicator für die Berichterstellung kann auf einem lokalen Server-Anwendungsknoten installiert werden.

Komponente	Mindestanforderungen	Erwünscht / empfohlen
Betriebssystem	Windows Server® 2008 R2	Windows Server 2008 R2 oder Windows Server 2012
Webserver	IIS Version 7.5	IIS Version 7.5 für Server 2008 R2 oder IIS Version 8 für Server 2012
Virtueller Speicher	8 GB	
COM+-Netzwerkzugriff	Nicht erforderlich	Nicht erforderlich
DTC-Netzwerkzugriff	Nicht erforderlich	Nicht erforderlich
Zugriffskomponenten	Erforderlich (mit Microsoft® .NET 4.5 Framework)	Erforderlich (mit Microsoft® .NET 4.5 Framework)
Microsoft .Net Framework	4.5.2	.NET 4.5.2
Datenbank-Server	Microsoft SQL Server® 2008 R2	SQL Server 2012
SQL-Authentifizierung	Erforderlich, mit Administratorrechten	Erforderlich, mit Administratorrechten
Serververwaltungsrechte	Erforderlich	Erforderlich

Allgemeine Voraussetzungen für die Implementierung

Die IT-Abteilung des jeweiligen Kunden muss für den lokalen Server von Digital Alternatives die folgenden Ressourcen bereitstellen.

SMTP (Postausgangsserver): Um Benachrichtigungen über den lokalen Server von Xerox® Digital Alternatives mit anderen Benutzern zu teilen, sind die SMTP-Server-Informationen des Kunden erforderlich Wenn der SMTP-Server eine Benutzerauthentifizierung erfordert, werden die Zugangsdaten des Service-Kontos verwendet. Der lokale Server nutzt die beim Kunden vorhandene SMTP-Schnittstelle für eine Verbindung zum MS Exchange-Mailserver des Kunden. In Digital Alternatives nimmt der SMTP-Server Verbindungen meistens auf Port 25 (TCP) entgegen. Dieser Wert kann aber während der Konfiguration des lokalen Servers in Übereinstimmung mit den Mailserver-Anforderungen des jeweiligen Kunden überschrieben werden.

LDAP-Verbindung für die globale Adresssuche: Die Suche im Benutzerverzeichnis des Kunden erfolgt hauptsächlich über diesen Server. Es wird damit im Rahmen von Registrierungen auf E-Mail-Adressen von Benutzern zugegriffen, um zu überprüfen, ob es sich um den rechtmäßigen Inhaber der jeweiligen Adresse handelt. Die globale Adresssuche wird ebenfalls damit durchgeführt. Wenn die IT-Abteilung des Kunden keine andere Port-ID vorgibt, wird der Standard-Port 389 (TCP) verwendet.

LDAP-Verbindung(en) für die Authentifizierung: Benutzer von Xerox® Digital Alternatives werden anhand der Netzwerk-Domänenauthentifizierung von Microsoft® Windows authentifiziert. Auf dem lokalen Server von Xerox® Digital Alternatives wird die Zugehörigkeit zu einer bestimmten Domäne (anhand des angegebenen Service-Kontos) automatisch erkannt, sodass Domänen und Server automatisch im Konfigurationsfenster angezeigt werden. Domänen und LDAP-Verbindungen können aber auch manuell hinzugefügt werden. Wenn die IT-Abteilung des Kunden keine andere Port-ID vorgibt, wird der Standard-Port 389 (TCP) verwendet.

Service-Konto: Die IT-Abteilung des Kunden muss ein Service-Konto anlegen, das von den drei Anwendungswartungsdiensten auf dem lokalen Server und den Anwendungspools in IIS genutzt werden kann. Die drei Wartungsdienste, die mit der Anwendung für den lokalen Server installiert werden, sind:

- Xerox.Digital.MaintenanceService – zur periodischen Löschung von Dokumenten, die von Benutzern von Digital Alternatives zum Löschen markiert wurden
- Xerox.Digital.QueueService – für die Interaktion mit MS Queuing zur Ausführung von Aufträgen
- Xerox.Digital.RelayService – für die Interaktion mit dem Zentralserver zum Abruf von Lizenzierungsdaten sowie als Schnittstelle zum Zentralserver für die Remote-Aktualisierung von Kundendokumenten

Bei diesem Konto muss es sich um ein Domänenkonto mit lokalen Administratorrechten auf den lokalen Server-Knoten von Xerox® Digital Alternatives handeln. Wenn der SMTP-Server eine Benutzerauthentifizierung erfordert, werden die Zugangsdaten des Service-Kontos verwendet. Das Passwort für dieses Konto sollte seine Gültigkeit nicht verlieren können, da ungültig gewordene Passwörter den lokalen Server beeinträchtigen. Die richtige Konfiguration des Service-Kontos auf dem lokalen Server von Xerox® Digital Alternatives können Sie dem entsprechenden Systemhandbuch entnehmen. Das Service-Konto muss zum Zeitpunkt der Installation auf dem lokalen Server vorhanden sein.

Internetzugang: Zugang zum Zentralserver von Xerox® Digital Alternatives ist erforderlich (HTTPS-Port 443).

Xerox® Digital Alternatives – Systemanforderungen für PC

Installation

Für eine erfolgreiche Installation müssen die folgenden Systemanforderungen erfüllt sein: (Je nach Konfiguration und Anforderungen des Systems kann zusätzliche Hardware erforderlich sein.)

- Unterstützte Betriebssysteme:
  - Windows® 7 (Professional, Ultimate, Enterprise)
  - Windows® 7 x64 (Professional, Ultimate, Enterprise)
  - Windows® 8
  - Windows® 8 x64
  - Windows® 8.1 (Professional, Ultimate)
  - Windows® 10 (Home, Pro, Enterprise)
- Prozessor vom Typ Intel® Pentium® 4 oder höher
- Arbeitsspeicher (RAM): mindestens 2 GB (4 GB empfohlen)
- Verfügbarer Festplattenspeicher: 250 MB für die Anwendung. Für gespeicherte Dokumente werden mindestens weitere 5 GB empfohlen.
  Hinweis: Bei sehr vielen Dokumenten ist ggf. noch mehr Speicherplatz erforderlich.
- Für alle unterstützten Betriebssysteme ist Microsoft® .NET Framework 4.5 erforderlich.

Sicherheit

- Die Client-Anwendung und der lokale Server von Digital Alternatives verwenden die Domänenauthentifizierung mit dem Active Directory des Kunden.
- Benutzer verwenden ihre Windows-Domänenanmeldung.
- Bei der PC-Client-Anwendung wird Internet Explorer für den Benutzer zum ersten Zugriff auf einen externen Zentralserver mit Proxy-Server-Einstellungen konfiguriert. Die Interaktion zwischen dem PC-Client und dem Zentralserver erfolgt über das HTTPS-Protokoll und Port 443. Der Proxy-Server des Kunden muss die Kommunikation über das HTTPS-Protokoll mit dem Zentralserver von Digital Alternatives während der Erstinstallation der PC-Client-Software zulassen.
- Zwischen dem lokalen Server von Xerox® Digital Alternatives und den Authentifizierungsservern des Kunden muss eine Verbindung hergestellt werden. Siehe den Abschintt „Allgemeine Voraussetzungen für die Implementierung“.

Hinweis: Nach der Installation ist Internetzugang erforderlich, um:

- die Client-Software von Xerox® Digital Alternatives beim Zentralserver und beim installierten lokalen Server erstmals zu registrieren.
- den Client von Xerox® Digital Alternatives erneut beim lokalen Server zu authentifizieren, falls dieser sich außerhalb des Netzwerks des Kunden befindet, wenn das Sicherheits-Token oder Kennwort des Clients ungültig geworden ist. Wenn die Client-Anwendung extern ausgeführt wird und kein Internetzugang besteht, zum Beispiel im Flugzeugmodus, lässt sich die Client-Software erst öffnen, wenn wieder eine Verbindung zum Internet oder zum internen Netzwerk des Kunden besteht.
  - Sicherheits-Token verlieren nach 8 Stunden ihre Gültigkeit.

Xerox® Digital Alternatives – Systemanforderungen für iPad

Installation

- Betriebssystem iOS 7, 8 oder 9
- iPad 2 und neuere Modelle, einschließlich von iPad mini™ (mit oder ohne Retina-Display). iPhone wird nicht unterstützt.

Sicherheit:

- Wird ein iPad als Client verwendet, wird die Domänenauthentifizierung mit dem Active Directory des Kunden genutzt.
- Zwischen dem lokalen Server von Xerox® Digital Alternatives und den Authentifizierungsservern des Kunden muss eine Verbindung hergestellt werden. Dies wird in einem anderen Abschnitt beschrieben.

Hinweis: Nach der Installation ist Internetzugang erforderlich, um:

a. Xerox® Digital Alternatives auf dem jeweiligen Client erstmalig zu registrieren.

b. den Client erneut zu authentifizieren, wenn das entsprechende Token oder Kennwort ungültig geworden ist.
   - Authentifizierungs-Token verlieren nach 8 Stunden ihre Gültigkeit.

c. Zur Synchronisierung und gemeinsamen Nutzung von Inhalten können Sie das Internet oder das Intranet des Kunden verwenden.

Xerox® Digital Alternatives – Systemanforderungen für Android

Installation

Unterstützte Hersteller von Android-Tablets und Betriebssystemversionen:

Gerät	Unterstützte Betriebssystem-Versionen
Asus Memo Pad 7	Version 4.4.2 (KitKat®)
Google (Asus) Nexus 9	Version 5.0 und 5.1.1 (Lollipop)
Google (Asus) Nexus 7	Version 4.1(Jelly Bean), 4.4.2 (KitKat®) und 5.0/5.1/5.1.1 (Lollipop)
Samsung Galaxy Tab 4	Version 4.4.2 (KitKat®)
Samsung Galaxy Tab S	Version 4.4.2 (KitKat®) und 5.0/5.1/5.1.1 (Lollipop)

Sicherheit:

- Wird ein Android-Gerät als Client verwendet, wird die Domänenauthentifizierung mit dem Active Directory des Kunden genutzt.
- Zwischen dem lokalen Server von Xerox® Digital Alternatives und den Authentifizierungsservern des Kunden muss eine Verbindung hergestellt werden. Dies wird in einem anderen Abschnitt beschrieben.

Xerox® Digital Alternatives – Systemanforderungen für Apple Macintosh

Installation

- Unterstützte Versionen des Apple-Betriebssystems: OS X 10.10 („Yosemite“) und OS X 10.11 („El Capitan“)

Sicherheit:

- Wird ein Apple Macintosh als Client verwendet, wird die Domänenauthentifizierung mit dem Active Directory des Kunden genutzt.
- Zwischen dem lokalen Server von Xerox® Digital Alternatives und den Authentifizierungsservern des Kunden muss eine Verbindung hergestellt werden.

4 Erwägungen zur Private Cloud

Hinweise für die Implementierung in Private Cloud

Einrichten einer B2B-Verbindung

Bei der Implementierung in der Private Cloud muss eine dedizierte B2B-Verbindung zwischen dem Netzwerk des Kunden und dem Netzwerk der Private Cloud von Xerox® eingerichtet werden, damit der in der Private Cloud gehostete lokale Server des Kunden mit dem Active Directory des Kunden kommunizieren kann. Außerdem ermöglicht die VPN-Verbindung zur Private Cloud die Kommunikation mit dem in der Private Cloud gehosteten lokalen Server genau so, als ober er im Netzwerk des Kunden installiert wäre. Eine typische Implementierung schließt eine VPN-Verbindung zwischen zwei Standorten ein, wodurch eine private Verbindung zwischen der Firewall des Kunden und der Firewall der Private Cloud gegeben ist. Zur Einrichtung einer effektiven VPN-Verbindung zur Private Cloud sind mehrere Punkte zu beachten.

IP-Adresse und Port-Nummer des Active-Directory-Servers des Kunden

Die bei der Registrierung verwendeten Zugangsdaten eines Benutzers werden vom Server der Private Cloud von Digital Alternatives mithilfe der LDAP-Schnittstelle via B2B-Verbindung an den Active-Directory-Server des Kunden übermittelt.

IP-Adresse und Port-Nummer der LDAP-Schnittstelle des Exchange-Servers des Kunden

Wenn sich Endbenutzer in Digital Alternatives das globale Adressbuch ihres jeweiligen Unternehmens anzeigen lassen, bezieht der lokale Server diese Informationen, indem er über die LDAP-Schnittstelle auf den Exchange Server des Kunden zugreift. Gewöhnlich wird Port 389 (TCP) verwendet, nach Vorgabe der IT-Abteilung des Kunden kann jedoch auch ein anderer Port gewählt werden.

Firewall-Regel für die Netzwerkadressübersetzung zur Änderung der IP-Adresse des Kunden

Da die von einzelnen Kunden für Netzwerkgeräte verwendeten internen IP-Adressen ggf. denen anderer Kunden bei Xerox ähneln, sollten Kunden eine NAT-Regel erstellen, um die IP-Adresse für den ausgehenden Datenverkehr mit dem Server der Private Cloud von Digital Alternatives zuzuordnen. Als Beispiel: Von den Netzwerkgeräten der Kunden werden zur internen Adressierung üblicherweise die Adressbereiche 192.168.1.XXX bzw. 10.10.1.XXX verwendet. Da die Client-Anwendungen aller Kunden mit dem Server der Private Cloud zur Synchronisierung von Dokumenten kommunizieren, sollte der gesamte ausgehende Datenverkehr des Kunden bei Xerox als einzelne Quell-IP-Adresse für eingehende Datenpakete angezeigt werden, die den gesamten Datenverkehr des Kunden zum Server der Private Cloud, mit dem eine Kommunikation erforderlich ist, darstellt.

Sicherheit von Dokumenten auf Cloud-basiertem lokalem Server

Alle in Digital Alternatives importierten Dokumente werden als unverschlüsselte PDF-Dateien im Dokumentenarchiv des lokalen Servers gespeichert. Auf dieses Archiv wie auch auf Anwendungs- und Datenbank-Server haben nur die für die Private Cloud von Xerox® zuständigen IT-Mitarbeiter Zugriff, da sie diese Server verwalten und warten. Der direkte Zugriff auf das Dokumentenarchiv durch Benutzer oder durch für die Private Cloud von Xerox® zuständige IT-Mitarbeiter ohne Zugriffsrechte wird mittels für das entsprechende Archiv angegebener Windows-Berechtigungen verhindert. So wenden wir bei der Speicherung von vertraulichen Dokumenten in Cloud-basierten Systemen im Hinblick auf die Sicherheit von Dokumenten und personenbezogene Daten sichere Methoden an.

Private Cloud – Physische Sicherheit

Xerox hostet seine Anwendungen und Daten in mehreren Rechenzentren und stellt auf diese Weise wesentliche technische Ressourcen als Reserve bereit. In allen Rechenzentren kommen physische Sicherheit, strenge Zugangsbestimmungen sowie Sicherheitsräume und -schränke zum Einsatz. Xerox trifft viele Sicherheitsvorkehrungen, damit vertrauliche Informationen von Kunden auch vertraulich bleiben. Xerox trifft administrative, technische und physische Sicherheitsvorkehrungen, um sicherzustellen, dass die Anforderungen des Kundenunternehmens an die Regelkonformität erfüllt werden.

- Zugang zu Rechenzentren über Zwei-Faktoren-Authentifizierung einschließlich von biometrischer Authentifizierung und Bewachung durch bewaffnete Sicherheitskräfte rund um die Uhr.
- Für Xerox wurde ein Bericht gemäß SSAE 16 Typ II erstellt.
- Die Speicher-Standorte verfügen über unterbrechungsfreie Stromversorgung und Backup-Systeme sowie Brand- und Hochwasserschutz.
- Die Rechenzentren, in denen die Private Cloud von Digital Alternatives gehostet wird, entsprechen den Normen ISO 27001, HIPAA und PCI-DSS sowie den Bestimmungen des SOX.
- Um die Sicherheit Ihrer Daten zu gewährleisten, überwachen wir unser Netzwerk permanent und führen regelmäßige Analysen der Sicherheit und des Einbruchsrisikos durch.
- Mehrere Internet-Backbone-Verbindungen ermöglichen Routing-Redundanz und eine Hochleistungsverbindung.
- Die Instanzen der Private Cloud von Digital Alternatives werden in den Rechenzentren von Xerox mit sekundären Standorten zur Notfallwiederherstellung gemäß ISO 27001 bereitgestellt.

Rechenzentren in Nordamerika		Rechenzentren in Europa	
Primärer Standort	**Sekundärer Standort (Notfallwiederherstellung)**	**Primäre Standorte**	**Sekundärer Standort (Notfallwiederherstellung)**
Lexington, KY, USA	Sandy, UT, USA	Telford, UK	Newport, UK
		Paris, FR	Tours, FR

Tabelle 2: Hosting-Standorte der Private Cloud

- Die sekundären Standorte werden dann in Betrieb genommen, wenn der jeweilige primäre Standort ausgefallen ist. Die Wiederherstellung erfolgt mithilfe der nächtlich erstellten Sicherungskopie des primären Standorts.
- Informationen und Dokumente von Kunden werden nicht in der Umgebung von Microsoft Azure gespeichert Alle in der Private Cloud von Digital Alternatives befindlichen Daten und Dokumente von Kunden werden in von Xerox verwalteten Rechenzentren gespeichert.
- Im Rechenzentrum für die Private Cloud werden folgende Klimaregelungen eingesetzt:
  - Umgebungskontrollen (Klimaanlage, Brandunterdrückung usw.)
  - Redundante Stromversorgung
  - Redundante Netzwerk-/Internetverbindungen (B2B und B2C)

Private Cloud – Zugangsverwaltung

Zu den Servern der Private Cloud erhalten nur solche Benutzer Zugang, die für die laufende Wartung der Server zuständig sind, und zwar nur bei Bedarf. Benutzer bei Xerox, die für die Wartung der Server der Private Cloud zuständig sind, beantragen Zugang beim Kontrollorgan für die Private Cloud, nachdem sie von ihrem Vorgesetzten die Genehmigung dazu eingeholt haben. Nachdem das Kontrollorgan für die Private Cloud die Anforderung geprüft hat, kann eine Genehmigung erteilt werden. Die Implementierung aller Benutzerzugriffe erfolgt durch ein vom Kontrollorgan bestimmtes Implementierungsteam. Der Zugriff auf die Datenbankinstanz und das Dokumentenarchiv eines Kunden ist auf eine Teilmenge derjenigen Benutzer beschränkt, die Zugriff auf die Private-Cloud-basierte Implementierung des Kunden haben.

Private Cloud – logische Zugriffsverwaltung

Für die Private Cloud von Xerox® wurden Rahmenbedingungen für die strategische Informationssicherheit geschaffen, die auf regelmäßigen Analysen der zahlreichen Bedrohungen, Schwachstellen und Auswirkungen auf den Betrieb beruhen, denen ein geschütztes Informationssystem ausgesetzt ist. Wir prüfen diese Rahmenbedingungen mindestens zweimal pro Jahr. Die Rahmenbedingungen beziehen sich auf die Informationssicherheit im gesamten Unternehmen sowie auf Sicherheitsaspekte, die für die Hosting-Umgebung der Private Cloud von Digital Alternatives typisch sind. Xerox nutzt eine Vielzahl von Vorgaben, Verfahren und Hilfsmitteln, um die permanente Einhaltung interner wie externer Sicherheitsrichtlinien zu gewährleisten.

Benutzer bei Kunden erhalten keine Benutzerkonten, die ihnen eine Remote-Anmeldung bei ihren gehosteten lokalen Servern erlauben würden. Die Berechtigung zur Anmeldung bei Servern der Private Cloud wird nur bestimmten Xerox-Benutzern erteilt, die zu Wartungszwecken Zugriff auf diese Server benötigen.

Private Cloud Identitätsbestätigung und Authentifizierung

In der Private Cloud von Digital Alternatives steht ein LDAP-Anschluss zur Verfügung, über den der gehostete lokale Server den unternehmenseigenen LDAP- bzw. Active-Directory-Server eines Kunden zur Benutzerauthentifizierung für Digital Alternatives nutzen kann.

Kunden, die sich in ihrer Client-Software bei Digital Alternatives anmelden, geben in der Client-Software ihre Zugangsdaten ein. Diese werden dann über die VPN-Verbindung zur Private Cloud an den lokalen Server übertragen. Der lokale Server authentifiziert dann die LDAP-Schnittstelle des Active Directory des Kunden über die VPN-Verbindung zur Private Cloud anhand der eingegebenen Zugangsdaten. Wenn der Active-Directory-Server des Kunden diese Zugangsdaten validiert hat, wird die Kommunikation der Client-Software des Kunden mit dem gehosteten lokalen Server zugelassen.

Private Cloud – Datenübertragung

Um zusätzlichen Datenschutz zu gewährleisten, werden die Daten bei der Übertragung an die bzw. von der Private Cloud von Digital Alternatives von Xerox verschlüsselt.

- SSL-Verschlüsselung bei Datenübertragung mit AES-256 auf Port 443.

Protokollierung und Prozessdatenspeicherung

Auf Verlangen kann Xerox Prüfberichte für die meisten Aktionen bzw. Aktivitäten in der Verwaltung von Digital Alternatives zur Verfügung stellen.

Zugriffe von Benutzern auf lokale Server werden in den Servern der Private Cloud mit der Standard-Benutzerprotokollierung von Windows protokolliert. In der Standardeinstellung werden diese Protokolle zwei Jahre lang gespeichert. Die Benutzerzugriffsdaten werden lokal auf dem lokalen Server gespeichert. Dafür sind etwa 80 MB Speicherplatz auf der Festplatte erforderlich.

Auf Verlangen kann Xerox dem Kunden die Benutzerzugriffsprotokolle in Textform bereitstellen.

Zeitüberschreitung

Die Benutzerauthentifizierung muss alle acht Stunden erneut vorgenommen werden. Wenn eine Sitzung in der Client-Software von Digital Alternatives abläuft, muss der Benutzer eine erneute Authentifizierung durchführen.

Anwendungssicherheit

Digital Alternatives wurde nach den Software-Entwicklungsstandards von Xerox entwickelt, die Design- und Code-Überprüfungen sowie Standard-Softwarebibliotheken wie Microsoft .NET einschließen.

Die gesamte Kommunikation zwischen den Komponenten von Digital Alternatives wird verschlüsselt, um die Kundendaten zu schützen.

IT-Notfallplanung

Um die Auswirkungen von Hardware-Störungen, temporären Ausfällen der Website, Naturkatastrophen und sonstigen Problemen möglichst gering zu halten, verfügt Xerox über redundante Hardware sowie Sicherungskopien Ihrer Daten. Jedes Jahr testen wir in einer Referenzinstallation von Digital Alternatives Pläne und Tools zur Datenwiederherstellung. Zur Datenwiederherstellung in Notfällen gehört auch die Failover-Standortzuordnung für jede Region, wie in der Tabelle der Rechenzentren definiert: Tabelle 2: Hosting-Standorte der Private Cloud.

5 Datenverwaltung und Datenschutz

Speicherung von Dokumenten

In Xerox® Digital Alternatives werden sämtliche Benutzerdokumente auf dem Dokumentenserver von Xerox® Digital Alternatives verwaltet. Neben lokalem Server und Datenbank-Server kann sich auch der Dokumentenserver von Xerox® Digital Alternatives entweder vor Ort befinden oder sicher in der Cloud von Xerox gehostet werden. Alle Dokumente werden unverschlüsselt auf dem Dokumentenserver von Xerox® Digital Alternatives gespeichert. Der Zugriff auf die Dokumente ist über Windows- und Serverzugriffsberechtigungen in der Domäne des Kunden geschützt und auf eine begrenzte Anzahl Mitarbeiter im Hosting-Rechenzentrum von Xerox beschränkt. Eine Schutzmaßnahme ist die Verschleierung von Dateinamen und -erweiterungen der gespeicherten Dokumente. Dokumente werden nicht automatisch, sondern von den Benutzern selbst gelöscht. Auch die Bereinigung von Dokumenten erfolgt nicht automatisch. Den einzelnen Benutzern steht eine bestimmte Menge an Speicherplatz für ihre Dokumente auf dem Dateiserver von Xerox® Digital Alternatives zur Verfügung. Dieser richtet sich nach dem in der Verwaltungsoberfläche festgelegten Benutzerkontingent. Auf dem Zentralserver von Xerox® Digital Alternatives werden dagegen keine Benutzerdokumente gespeichert.