WHITE PAPER

Sieben strategische Vorgaben für die Auswahl einer modernen Filesharing- und Content-Collaboration-Lösung für Unternehmen

Unternehmenslösungen für Dateiaustausch und -synchronisierung (Enterprise File Sync and Share = EFSS) sind zu leistungsstraken Plattformen der Steuerung von Geschäftsabläufen und Innovationen herangereift.

syncplicity by axway

Inzwischen haben wir uns an die Cloud gewöhnt. Wir speichern ohne weitere Gedanken unsere Familienfotos, die Termine für das Fußballtraining der Kinder und die Lieblingsrezepte auf Dropbox und OneDrive. Es überrascht also nicht, dass manche Firma meint, diese Angebote seien auch für das Unternehmen geeignet. Denn wenn die Anbieter auch Lizenzen für Unternehmen verkaufen, sollten sich diese schließlich auch für den geschäftlichen Einsatz eignen, oder?

Manchmal ist dies auch der Fall. Die üblichen Lösungen für Dateisynchronisierung und -austausch, die auch von den Mitarbeitern daheim genutzt werden, sind durchaus auch für Unternehmen geeignet, sofern Sicherheitsfragen oder regulatorische Anforderungen keine Rolle spielen.

Wir übrigen brauchen jedoch eine sichere Lösung, die von Grund auf für den geschäftlichen Einsatz konzipiert wurde. Aktuelle Erfahrungen und Arbeitsweisen zur Produktivitätssteigerung sowie die Gewährleistung von Sicherheit und Compliance machen eine auf Unternehmen zugeschnittene Architektur unabdingbar.

Einfaches Filesharing ist out

Viele Unternehmen unterschätzen die Komplexität bei den Anforderungen für Dateisynchronisierung und -austausch. Schließlich will man ja nur Dateien verschieben. Das sollte doch einfach genug sein.

Tatsächlich muss eine EFSS-Lösung aber genauso komplex sein, wie das Unternehmen, dem sie dient. Außerdem entwickeln sich Unternehmen mit rasanter Geschwindigkeit. In den letzten paar Jahren mussten typische Unternehmen bereits zahlreiche Veränderungen bei den geschäftlichen und technologischen Praktiken umsetzen. Heute ist die digitale Transformation eine Grundvoraussetzung um konkurrenzfähig zu bleiben, weshalb die Unternehmen sich auf die Überführung all ihrer Prozesse vom Papier in die digitale Form konzentrieren. Sie erwarten mehr von ihren EFSS-Systemen als nur Filesharing und Dateisynchronisation. Sie brauchen leistungsstarke und hochentwickelte Methoden, um die Zusammenarbeit, Richtlinien und Speicheroptionen zu managen. Dieser Trend ist so ausgeprägt, dass Gartner den EFSS-Bereich inzwischen neu als Content-Collaboration-Platform-Bereich definiert. Als Abkürzung für Content Collaboration Platform wird im übrigen Dokument CCP verwendet.

Um festzustellen, ob eine CCP-Lösung die strategischen Unternehmensziele unterstützt, sollten IT-Leiter sieben Kernkriterien berücksichtigen.

Sieben Kriterien für die Auswahl einer modernen CCP-Lösung

Vor wie vielen dieser Herausforderungen stehen Sie heute?

- ☐ Zunahme des Cloud-Computing
- ☐ Kosten für Altdatenspeicherung
- ☐ Infrastruktur für Altdaten — Dateiserver
- ☐ Sicherheit und Schutz der Daten
- ☐ Hoheit und Kontrolle über die Daten
- ☐ Digitale Mitarbeiter auf der ganzen Welt
- ☐ Schatten-IT
- ☐ Programme auf eigenen Geräten von Mitarbeitern
- ☐ Sicheres internes und externes Filesharing

Wenn Sie in einem der Kästchen eine Haken machen, brauchen Sie eine moderne, für Unternehmen ausgelegte CCP-Lösung.

01

Benutzerfreundlichkeit

Die Benutzerfreundlichkeit beginnt beim Design. Bei einer CCP-Lösung sollte das Design unsichtbar sein. Die Benutzer sollten normal arbeiten können, ohne Dateien bewusst synchronisieren oder freigeben zu müssen. Das sollte von allein gehen.

Eine Lösung mit schlechtem Design verärgert die Benutzer und, noch wichtiger, verringert die Produktivität. Tatsächlich geben 57 % der Büroangestellten an, dass sie eine Stunde pro Tag nach fehlenden Dokumenten suchen.[1] Diese können sich auf der Festplatte oder, schlimmer noch, im persönlichen Dropbox- oder OneDrive-Speicher eines anderen Mitarbeiters befinden.

Wird den Mitarbeitern keine praktikable Unternehmenslösung angeboten, neigen sie dazu, die Tools zu nutzen, die sie privat bevorzugen. Sie haben keine bösen Absichten, aber ihr Handeln birgt Risiken. Außerhalb des Netzwerks gespeicherte Dokumente sind effektiv für das Unternehmen verloren und wenn sie beim persönlichen Filesharing-Dienst eines Mitarbeiters liegen, könnten sie über ein wiederverwendetes oder ungeeignetes Passwort zugänglich sein, das bereits im Darknet zum Verkauf steht.

In vielen Unternehmen benötigen extern arbeitende Mitarbeiter Zugriff auf Unternehmensdaten über ein virtuelles privates Netzwerk (VPN). Über das VPN können sie zwar auf Dateien zugreifen, aber es unterstützt die für eine hohe Produktivität essenziellen Arbeitsabläufe bei Zusammenarbeit und Automation nicht.

Mitarbeiter brauchen einen Dateizugang über eine App, mit der sie Daten streamen und gemeinsam nutzen können, ohne sich anzumelden und ohne Dateien herunterzuladen oder per E-Mail zu verschicken. Diese Funktionalität fördert die modernen neuen Arbeitsweisen, die dabei helfen, die von der digitalen Transformation erwarteten Produktivitätssteigerungen zu erreichen.

Grundlagen für die Produktivität

- ☐ Zugang zu sämtlichen Unternehmensdaten
- ☐ Sicherheit bei Filesharing und Datenempfang
- ☐ Einmal synchronisieren, überall verfügbar
- ☐ Sicherheit bei Filesharing und Zusammenarbeit mit externen Parteien
- ☐ Kein „magischer“ Ordner erforderlich
- ☐ Echtzeit-Backup
- ☐ Vorhersagende Analysen
- ☐ Mobile Apps auf Endkundenniveau
- ☐ Offline-Zugriff
- ☐ Automatische Versionskontrolle und Wiederherstellungsfunktionen

1 Figueiredo, Debora. „Verschwenden Sie die Arbeitszeit der Mitarbeiter?“ Developing People Globally. 24. März 2016.

02

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) sorgt in Unternehmen weltweit für große Verwirrung. Manche glauben, die neue Verordnung wäre nur für Unternehmen mit Sitz in der EU relevant, doch das ist eine gefährliche Fehlannahme. Unternehmen außerhalb der EU müssen sie ebenfalls einhalten, selbst wenn sie mit nur einem Unternehmen oder sogar einer einzelnen Person innerhalb der EU Geschäfte machen. Die Strafen für Verstöße sind streng: das Strafmaß am unteren Ende beträgt zwei Prozent der weltweiten Einnahmen oder 10 Millionen Euro (der größere Betrag kommt zur Anwendung) und am oberen Ende sind es vier Prozent oder 20 Millionen.

Um Strafen zu vermeiden, benötigen die Unternehmen die Hoheit über ihre Daten. Hinter der Datenhoheit steckt das Konzept, dass Daten den Gesetzen desjenigen Landes unterliegen, in dem sie gespeichert sind. Dies kann eine Herausforderung für ein vernetztes Unternehmen sein, das seine Geschäfte zum großen Teil über die Cloud und auf virtuellen Maschinen abwickelt.

Eine DSVGO-konforme CCP-Lösung muss dem Kunden die Wahl des SaaS-Standortes für die Speicherung der Metadaten und für die eigentlichen Daten ermöglichen, ob in Azure, AWS, vor Ort oder in einer hybriden Speicherumgebung.

Für eine DSGVO-konforme CCP-Lösung ist zwingend vorgeschrieben, dass es keinerlei Kenntnis des Dateninhalts gibt. Das bedeutet, dass ein Anbieter die Kundendaten so verschlüsselt, dass diese nur vom Kunden und niemals vom Anbieter oder von Drittten gelesen werden können. Diese Sicherheitsarchitektur unterstützt die DSGVO-Konformität, indem sie Unternehmensdaten vor nicht autorisiertem Zugriff schützt, egal ob durch böswillige Einzelpersonen oder auf Anordnung einer Regierung.

Um die Anforderungen der DSGVO zu erfüllen, brauchen Unternehmen eine Lösung, die rollenbasierte Sicherheitsrichtlinien unterstützt und regelt, welche Daten zugänglich sind und ausgetauscht werden dürfen. Die Lösung sollte sich auch in die führenden Datenschutzlösungen einbinden lassen, um das Verlustrisiko für *personenbezogene Daten* und *geschützte Gesundheitsdaten* zu minimieren.

Speicherung On-premise und private Speicherung sollten möglich sein. Viele Unternehmen mit Sitz in der EU bevorzugen die Datenspeicherung On-premise, um sicherzustellen, dass private Kundendaten auf dem Territorium der EU gespeichert werden.

DSGVO, personenbezogene Daten und geschützte Gesundheitsdaten

Obwohl die drei großen Behörden für die gesetzlichen Anforderungen viele Ähnlichkeiten aufweisen, sind sie nicht völlig deckungsgleich. Wenn Ihre CCP-Lösung sich für eines der Regelwerke für die Daten eignet, ist sie wahrscheinlich auch für die anderen geeignet. Fragen Sie bei Ihrem Anbieter, wie dessen Lösung Sie bei der Einhaltung der Richtlinien unterstützt.

Syncplicity verleiht Ihnen die Hoheit über Ihre Daten

Syncplicity verfügt über eingebaute Standortkontrolle, mit der Kunden wählen können, wo die Daten gespeichert werden sollen. Anwender brauchen nie zweimal darüber nachzudenken, auf welche Region sie zugreifen. Mit nur einer Anmeldung erhalten sie Zugriff auf beide und der Standort der Daten ist immer unsichtbar.

03

Ransomware

Noch vor Kurzem war Ransomware eine Methode, mit der Kleinkriminelle mit ein paar Programmierkenntnissen einige Bitcoins ergatterten. Binnen kurzer Zeit hat sich Ransomware jedoch zu einer weit schlimmeren Bedrohung entwickelt: Nationalstaaten mit strategischen Agenden nutzen Ransomware-Angriffe. Diese Nationalstaaten wollen keine Kryptowährungen – sie wollen den Handel manipulieren. Manche Analysten glauben sogar, dass WannaCry und Petya mehr waren als Malware-Angriffe – nämlich Tests für Cyberwaffen.

Unternehmen sind zu Recht besorgt über Ransomware, denn nach Angaben von Cisco nimmt Ransomware jährlich um 350 Prozent zu. Dabei macht das Lösegeld nur einen Teil der Kosten aus. Fehlerbeseitigung, Strafzahlungen, Prozesskosten und die Entschädigung der Kunden sind weitere Posten die sich schnell summieren. Darüber hinaus wird ein Unternehmen, das einmal gezahlt hat, schnell als gutes Ziel bekannt, das weitere Hacker und noch mehr Ransomware-Angriffe anzieht.

Ransomware entwendet keine Daten, sondern verschlüsselt sie derart, dass der rechtmäßige Eigentümer sie nicht mehr nutzen kann. Die gute Nachricht dabei ist allerdings, dass es eine einfache Methode gibt, die Ransomware relativ harmlos macht: Sicherheitskopien der Dateien.

Überraschenderweise sind viele Unternehmen gerade darin nicht besonders gut. Sie glauben, es sei sicher genug, sich auf den Schutz der Netzwerkperimeter zu verlassen. Aber in den meisten Unternehmen sind erhebliche Mengen unstrukturierter Daten hier und dort über Netzwerke und Endpunkte verstreut.

Vielleicht hat ein Finanzanalyst ein PDF auf einem mobilen Gerät oder ein Wissenschaftler hat sensible Forschungsdokumente im Papierkorb auf seinem Desktop.

Eine unternehmensweite CCP-Lösung macht den Sorgen um Ransomware ein Ende. Sie kann zwar Ransomware-Angriffe nicht verhindern, was aber für jede Sicherheitslösung gilt, denn wie heißt es so schön: „Ein Hacker braucht nur einmal einen Glückstreffer zu landen." Jedoch geht der Angriff ins Leere, weil das Unternehmen die Dateien ersetzen und wiederherstellen kann. Unternehmen, die so vorgesorgt haben, können Hackern die kalte Schulter zeigen, denn die beim Angriff verschlüsselten Dateien sind nur noch nutzlose Nullen und Einsen, die nicht gegen den rechtmäßigen Eigentümer eingesetzt werden können.

Syncplicity hilft branchenübergreifend bei der Entschärfung von Ransomware

- Ein von Petya betroffenes weltweites Pharmaunternehmen nutzte Syncplicity zur schnellen Wiederherstellung.
- Ein global agierendes Luftfahrtunternehmen sparte drei Millionen Dollar bei der Backup-Software ein, indem es Syncplicity einführte.
- Ein führender Mikrochiphersteller schützt über 100.000 Laptops von Mitarbeitern mit Syncplicity.

Eine CCP-Lösung, die Dateien bereits im Rahmen ihrer Kernfunktionen repliziert und wiederherstellt senkt die Ausgaben für Backup-Software und verkürzt die Wiederherstellungszeiten. Das wiederum reduziert Kosten und entgangene Umsätze durch Ausfallzeiten nach Ransomware-Angriffen.

04

Zwangsabhängigkeit vom Cloud-Anbieter

Eine Zwangsabhängigkeit vom Cloud-Anbieter liegt vor, wenn ein Unternehmen einen Teil der Geschäftsaktivitäten in die Cloud verlagert hat und dort nicht mehr herausbekommt, weil die Migration zu aufwändig wäre. Das Alt-System lässt sich nicht einfach in die neuen Lösungen integrieren oder die Daten des Alt-Systems sind so strukturiert, dass die Vollständigkeit der Migration ungewiss ist. Vielleicht werden wirklich alle Dateien verschoben, vielleicht aber auch nicht.

Unternehmen sollten nur CCP-Lösungen in die engere Wahl ziehen, die bei der Auswahl der Art des Speichers unabhängig sind. Dabei geht es nicht nur um die Wahl des Anbieters, sondern auch darum, ob in der Cloud, On-premise oder hybrid gespeichert wird. Diese Flexibilität ist grundlegend für die Agilität des Unternehmens, welche durch eine Lösung weiter gestärkt wird, die automatische Migration ermöglicht.

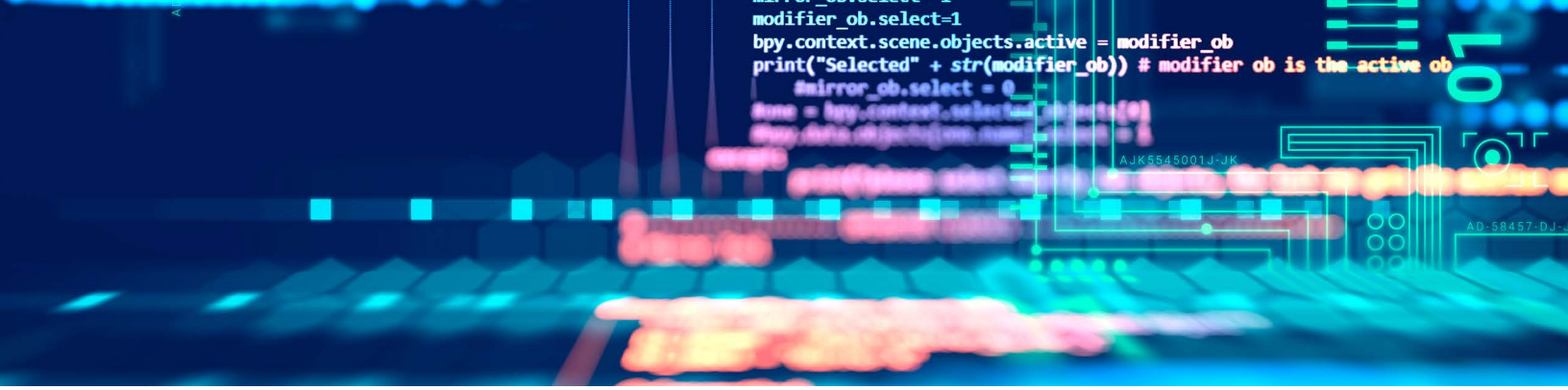
Ein typischer Fall ist die DSGVO. Unternehmen mit Sitz in der EU, die Datenzentren in den USA nutzen, müssen nun alle ihre Daten auf Server in der eigenen Region verlagern. Diejenigen mit einer sicheren CCP-Lösung können die Daten an einem normalen Werktag und ohne unternehmensweite Anstrengungen verschieben.

Ein alltäglicheres Anwendungsszenario wäre die Entscheidung eines Unternehmens z. B. von AWS auf Azure umzusteigen. Eine CCP-Lösung muss mit beiden Systemen funktionieren und der Übergang muss nahtlos erfolgen oder das Unternehmen büßt an Produktivität ein, weil sich die Mitarbeiter erst an neue Anmeldedaten und Arbeitsabläufe gewöhnen müssen. Das treibt außerdem die Kosten in die Höhe und das IT-Team muss die Anrufe von frustrierten Anwendern bewältigen.

Es ist von strategischem Vorteil, den Anbieter zu wechseln, wenn das Vertragsende naht oder der Vertrag neu ausgehandelt werden muss. Hat ein Unternehmen die Kontrolle über die eigenen Daten, kann der Anbieter gewechselt werden, ohne den Betrieb zu unterbrechen, falls die neuen Bedingungen nicht zufriedenstellend sind.

F.: Bei wem wurde weltweit die größte und schnellste CCP-Lösung bereitgestellt?

A.: Die Antwort lautet Siemens. Dort spart man 24 Millionen Dollar pro Jahr durch die Konsolidierung von Speicher mit Hilfe von Syncplicity.



05

Externer Datenaustausch

Der Austausch von Daten über die eigenen vier Wände des Unternehmens hinweg erfordert umfassendere Sicherheitsmaßnahmen als rein interner Datenaustausch. Dies trifft insbesondere dann zu, wenn sensible Daten geteilt werden und gesetzliche Vorgaben existieren.

Sicherheit und Compliance sind für die meisten Unternehmen wichtig, aber manche sind stärker belastet als andere. Unternehmen der Finanzwirtschaft verarbeiten große Mengen personenbezogener Daten, Produzenten und Unternehmen der Biowissenschaften müssen ihr intellektuelles Eigentum schützen und Unternehmen im Gesundheitswesen tragen die Verantwortung für die Art von Daten, die im Darknet als wertvollstes Handelsgut gelten: geschützte Gesundheitsdaten.

Sicherheit hat bei den meisten Unternehmen höchste Priorität, ist aber nicht die einzige Sorge. Die Benutzerfreundlichkeit muss gewahrt werden und zwar innerhalb und außerhalb des Unternehmens. Ein unbefriedigendes Benutzererlebnis kann bereits an sich zu einem Sicherheitsrisiko werden, denn wenn die Benutzer die unternehmenseigenen Tools nicht mögen, finden sie Wege, diese zu umgehen. Dateien landen auf persönlichen Filesharing-Accounts, auf USB-Sticks oder Festplatten, wo sie für das Unternehmen effektiv verloren sind.

Ein Unternehmen, das Daten mit Geschäftspartnern austauscht sollte auf vier Faktoren achten:

1. Sicherer und benutzerfreundlicher, externer Datenaustausch mit reibungsloser Einbindung der externen Benutzer
2. Keine Zusatzkosten für externen Datenaustausch
3. Kontrollfunktionen für den Datenaustausch mit Partnern für volle Kontrolle des Unternehmens über die Vertrauensstufen der einzelnen Geschäftspartner
4. Rechtemanagement und Vorbeugung gegen Datenverlust zur Vermeidung einer versehentlichen oder böswilligen Weitergabe sensibler Daten

Diese vier Faktoren machen den Umgang mit der CCP-Lösung für alle Benutzer einfacher, was zu höherer betrieblicher Effizienz führt, die bei komplexen Netzwerken einen bedeutenden Einfluss haben kann.

„Externes Filesharing ist für die Texas A&M University von kritischer Bedeutung. Die neuen Kontrollmöglichkeiten von Syncplicity von Axway geben mir die Gewissheit, dass meine Teams ihre Dateien und Ordner sicher innerhalb der vertrauenswürdigen Gruppe unserer Organisationen gemeinsam nutzen können. In der digitalen Welt von heute ist die Firewall nicht mehr die Grenze für die gemeinsame Nutzung von Daten und Informationen. Durch diese Verbesserungen können wir den Datenzugriff auf eine vertrauenswürdige Gruppe von angeschlossenen Organisationen begrenzen, was uns bei der Sicherheit und Einhaltung der Compliance hilft, während wir die zentrale Kontrolle behalten und eine einfache Zusammenarbeit der Endnutzer ermöglichen.“

Danny Miller, CISO System Chief Information Security Officer an der Texas A&M University

06

Zusammenarbeit zwischen Maschinen

Automation ist inzwischen kein Wettbewerbsvorteil mehr, sondern lebensnotwendig. Unternehmen erwarten, dass ihre Mitarbeiter und Partner mit automatisierten Anwendungen, Systemen und Geräten interagieren. Dasselbe sollten sie von ihren CCP-Lösungen fordern.

Aber viele CCP-Lösungen sind nicht fähig, Zusammenarbeit zwischen Maschinen zu unterstützen. Menschen müssen eingreifen, um unstrukturierte Dateien in die CCP-Lösung und wieder aus ihr hinaus zu befördern. Dies schmälert die betriebliche Effizienz, strapaziert die Ressourcen und beeinträchtigt das Benutzererlebnis.

Stellen Sie sich zum Beispiel eine Bank vor, die einem Immobilienkäufer einen Antrag für eine Hypothek übermittelt. Eine CCP-Lösung, die nicht mit Maschinen zusammenarbeitet, kann dazu führen, dass der Kreditnehmer zuerst Dokumente von einem System herunterladen, dann in eine Lösung für die sichere Unterzeichnung hochladen und danach das unterzeichnete Dokument an den Sachbearbeiter und den Bürgen weiterleiten muss. Eine automatisierte CCP-Lösung übernimmt den Großteil dieses Arbeitsablaufs und stellt Dokumente zwischen Käufer und Finanzinstitut automatisch einfach per Mausklick zu.

In anderen Anwendungsszenarios könnte ein Kernspintomograf die Aufnahmen eines Patienten automatisch an den Radiologen, den Hausarzt und die Versicherung übermitteln. Ein Pilot könnte die Meldungen von IdD-Sensoren des Flugzeugs direkt an die Bodencrew weiterleiten, sodass bei der Landung die entsprechenden Ersatzteile bereitstehen.

Effizienzsteigerungen wie diese erfordern ein ausgeklügeltes CCP-System mit fortschrittlicher Dateiweiterleitung, automatischer Integration bereits vorhandener und kundenspezifischer Anwendungen und API-basierter Integration der gängigen Cloud-Anwendungen.

Automation ist mit gemeinsamer Datennutzung leistungsstärker

In ihrer Branche führende Unternehmen haben Syncplicity in ihre automatisierten Prozesse eingebunden. Das Ergebnis?

- Verbesserungen bei betrieblicher Effizienz und Kundennutzen
- Bessere Nutzung der Ressourcen bei IdD-Anwendungsszenarien
- Vorhandene Systeme werden flexibel
- Vorhandene Systeme erhalten externe Filesharing-Funktion
- Vorhandene Systeme erhalten Cloud-basierte Verteilungsfunktionen

07

Kundenerfolg

Der Kundenerfolg hängt von zwei Gruppen ab: den Benutzern und dem IT-Team. Ein CCP-Anbieter sollte ein Kommunikationsprogramm auf Basis des Anwendungsszenarios und der Unternehmensziele anbieten, um die Benutzerakzeptanz zu erhöhen. Das Programm sollte nicht der einmaligen Anwendung dienen, sondern die Grundkenntnisse der Benutzer weiterentwickeln. Die Lösung sollte über Reportingfunktionen verfügen, die es ermöglichen, Nutzungsmuster einzusehen und nachzuverfolgen, um dem Unternehmen Erkenntnisse zur Leistung der CCP-Lösung zu liefern.

Das IT-Team wird Hilfe dabei benötigen, die Funktionen der CCP-Lösung zu verstehen. Die Implementierung sollte mit einer Überprüfung der Anwendungszenarien, Sicherheit und Infrastruktur im Unternehmen beginnen. Die Ergebnisse sollten dazu genutzt werden, Erfolgskriterien aufzustellen und einen Projektplan zu entwickeln, der die Anforderungen abdeckt. Erst dann ist das System bereit für die Konfiguration, Inbetriebnahme und Nutzung.

Der Schlüssel zum Erfolg für den IT-Leiter

- Die Benutzerakzeptanz ist kritisch für den Erfolg und die Amortisation, doch das ist nicht der einzige Faktor. Die IT-Leiter müssen bei der Auswahl einer CCP-Lösung die zunehmenden Compliance-Anforderungen und eine immer düstere Bedrohungslandschaft berücksichtigen.
- Unternehmen mit sensiblen Anforderungen im regulatorischen, sicherheitstechnischen oder Lieferkettenbereich benötigen CCP-Lösungen, die von Grund auf für Unternehmen konzipiert sind. Systeme für Konsumenten, die inzwischen als Unternehmenslösungen angeboten werden, besitzen keine Funktionen für Auditing und Verschlüsselung.
- Im Markt der CCP-Lösungen sind Zwangsabhängigkeiten vom Anbieter zunehmend die Regel. Unternehmen sollten die Gewissheit haben, ihre Daten jederzeit an jeden beliebigen Ort verschieben zu können.
- Eine Zusammenarbeit über die eigenen vier Wände des Unternehmens hinaus mit Kunden, Patienten, Lieferanten und Auftraggebern ist erheblich anspruchsvoller als rein internes Filesharing. Wählen Sie eine Lösung, die sicher genug ist, diese Anforderungen zu erfüllen.
- Fortschritte bei der Automation sowie Integration in Unternehmensanwendungen und IdD-Anwendungsszenarien lassen CCP immer schneller über die Grenzen der menschlichen Zusammenarbeit hinauswachsen. Wählen Sie eine Lösung, die dafür ausgelegt ist, bei ihrer Evolution in den nächsten paar Jahren optimalen Nutzen aus der Technologie zu ziehen.

Reibungsloses Onboarding mit Syncplicity

Vorbereitung der IT-Teams. Syncplicity bietet ein Paket für die Vorbereitung der IT-Mitarbeiter an, mit dem die IT-Abteilungen in Syncplicity geschult werden. Es hilft, Sicherheits- und Verwaltungskontrollen einzurichten und stellt sicher, dass die Compliance-Vorgaben eingehalten werden.

Einbindung der Nutzer. Syncplicity hilft bei der Anwenderakzeptanz, indem die Unterstützung und Anleitung auf Basis von bewährten Praktiken und Marketingaktivitäten bereitgestellt werden. Zum Bespiel durch Einführungskampagnen mit E-Mails, Auftaktveranstaltungen sowie Tipps und Tricks.