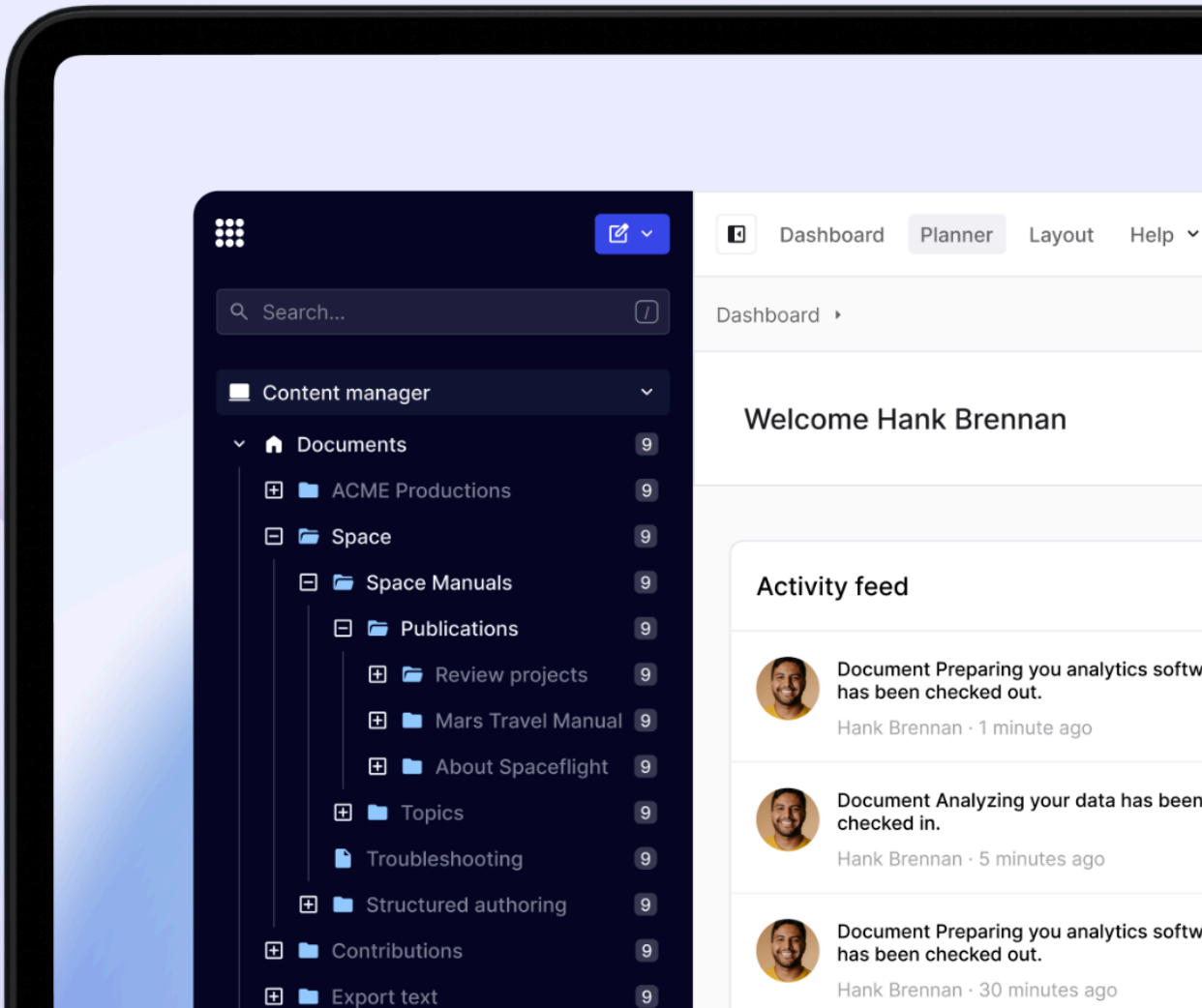
paligo

Von On-Premise zur Cloud: Nutzen Sie cloudbasiertes Component Content Management



I. Zusammenfassung

Viele Unternehmen, insbesondere in den Bereichen Pharma, Finanzdienstleistungen und Fertigung, glauben noch immer an einen erheblichen Vorteil von On-Premise-Lösungen für das Component Content Management (CCM) gegenüber „Off-Premise“-Lösungen, also Cloud- oder SaaS-Lösungen (Software-as-a-Service).

Häufig werden in diesem Zusammenhang folgende Vorzüge einer bestehenden – oder sogar neu angeschafften – On-Premise-Lösung genannt:

Sicherheit

Individuelle Anpassung

Geschwindigkeit/Latenz

Preiskontrolle

Zuverlässige Verbindung

Doch die im Vorfeld getätigten Investitionen und die Ressourcen, die für die Implementierung, Wartung und Aktualisierung/Migration einer On-Premise-Lösung für Content Management laufend erforderlich sind, zeigen schnell, dass sich diese nur selten lohnt, wenn man mittel- bis langfristig die Risiken gegen die Vorteile abwägt. Letztendlich ist keine Lösung risikolos. Wie kann man diesen Aufwand dann als angemessene Geschäftskosten rechtfertigen?

Ungeachtet einiger bekannter Nachrichten über Hacking-Vorfälle kann jedes Unternehmen einer beliebigen Branche mithilfe der richtigen Sicherheits- und Datenschutzverfahren und eines zuverlässigen, vertrauenswürdigen Anbieters eine SaaS-Lösung für das Component Content Management nutzen, ohne sich Sorgen über Datenschutzverletzungen oder Datenverluste machen zu müssen.

In diesem Whitepaper werden die Nuancen von lokalen und cloudbasierten CCMS-Lösungen untersucht. Wir beleuchten die Vorteile und Herausforderungen, die mit

den Hauptmerkmalen einer Hosting-Umgebung verbunden sind, und verdeutlichen, warum cloudbasierte Plattformen zunehmend zur bevorzugten Wahl zukunftsorientierter Unternehmen werden.

Darüber hinaus bschäftigen wir uns mit einigen speziell in Deutschland gegebenen Anforderungen und gehen auf wichtige Überlegungen für die Arbeit mit einem cloudbasierten CCMS ein.

II. Einleitung

Die effektive Verwaltung der technischen und geschäftlichen Dokumentation ist ein entscheidender Unternehmensaspekt. Ganz gleich, ob es sich um Produkthandbücher, technische Anleitungen, regulatorische Dokumente oder Standardarbeitsanweisungen handelt: Entscheidend ist, dass das Unternehmen aktuelle Unterlagen und Informationen schnell und effizient organisieren, aktualisieren und verteilen kann. Diese Notwendigkeit wird in Branchen, in denen Compliance, Genauigkeit und Pünktlichkeit unumstößliche Voraussetzungen sind, noch wichtiger.

Ein Component Content Management System stellt eine Methode des Content Authoring und Content Managements dar, bei der Informationen in diskrete, wiederverwendbare Komponenten zerlegt werden (strukturiertes Authoring).Diese Komponenten, wie Topics, Absätze, Text-Snippets und Bilder, werden in einem zentralen Repository gespeichert und können dynamisch zusammengestellt werden, um verschiedene Dokumentationen zu erstellen, die auf unterschiedliche Zielgruppen, Kanäle oder Kontexte zugeschnitten sind.

Component Content Management Systeme gibt es in verschiedenen Formen, die alle unterschiedliche Vorteile und zu berücksichtigende Faktoren haben. In der Vergangenheit haben Unternehmen On-Premise-Lösungen bevorzugt, bei denen Software und Daten in der Infrastruktur des Unternehmens gespeichert sind. Diese Lösungen bieten ein Gefühl der Kontrolle über Sicherheit, Kundenanpassung und Konnektivität, das lange als unerlässlich für sensible oder geschäftskritische Inhalte galt.

Die Landschaft hat sich jedoch weiterentwickelt. Die Entstehung von cloudbasierten oder SaaS-Systemen (Software-as-a-Service)für das Component Content Management (CCMS) führte zu einem Paradigmenwechsel bei der Herangehensweise der Unternehmen an das Content Management. Cloudbasierte CCMS-Plattformen nutzen Remote-Server und Internetkonnektivität für skalierbare, flexible und kostengünstige Lösungen. Trotz anfänglicher Befürchtungen hinsichtlich Sicherheit und Kontrolle bieten cloudbasierte Plattformen zahlreiche Vorteile, welche die Bedenken überwiegen.

SaaS ist das größte Cloud-Computing-Segment und ein Standard-Bereitstellungsmodell für Unternehmen. Der SaaS-Markt wird 2024 voraussichtlich 282,20 Milliarden US-Dollar erwirtschaften, davon 69,82 Milliarden US-Dollar in Europa.

Quelle: Statista

Im nächsten Abschnitt führen wir eine Vergleichsanalyse des cloudbasierten und des On-Premise-CCMS durch, wobei wir uns auf die Hosting-Umgebung der jeweiligen Lösung (Hardware, Software, Infrastruktur) konzentrieren.

Bevor wir fortfahren, soll darauf hingewiesen sein, dass wir den Begriff cloudbasiertes CCMS sowohl für SaaS-CCMS als auch für CCMS mit Cloud-Hosting verwenden.

III. Vergleichsanalyse: On-Premise-CCMS im Vergleich zu cloudbasierten CCMS

Betrachten Sie zunächst die folgende Tabelle an, in der die Unterschiede zwischen einem On-Premise- und einem cloudbasierten CCMS hervorgehoben werden.

Hinweis: Sie können das Whitepaper entweder vollständig bis zum Ende durchlesen oder über einen der Links in der Tabelle zu dem jeweiligen Abschnitt springen.

Aspekt/Leistungsmerkmal	On-Premises	Cloud/SaaS
Sicherheit	Verantwortlich für die gesamte Sicherheit, einschließlich Netzwerk, Hardware und Software, Benutzerzugriff und -authentifizierung, Sicherheitsschulung, Überwachung und Wiederherstellung.	Der CCMS-Anbieter sorgt für Sicherheit in der Cloud-Umgebung, unter anderem mit erweiterter Verschlüsselung, Identitäts- und Zugriffsmanagement sowie mit Bedrohungserkennungssystemen. Entspricht in der Regel Sicherheitszertifizierungen wie ISO 2001 oder SOC 2.

Kosten	Verantwortlich für die Bezahlung der gesamten Umgebung, einschließlich Server, Software und CCMS-Lizenzen, sowie für die Ressourcenschulungen und die laufende Wartung	Sie bezahlen nur für ein Abonnement, in der Regel ein Jahresabonnement, das alle Kosten abdeckt, einschließlich Umgebung, CCMS und Support.
Skalierbarkeit	Einrichtung für eine künftige Erweiterung, Vorauszahlung für eine künftige Erweiterung oder Einrichtung für die aktuellen Erfordernisse und Erweiterung je nach Bedarf, mit dem Risiko, dass der Speicherplatz nicht ausreicht oder sich die Leistung verschlechtert.	Automatische Skalierung von Speicherplatz und Leistung je nach Bedarf ohne Auswirkungen für Ihre Endbenutzer. Erweiterung in Zeiten mit hohem Geschäftsvolumen oder Reduzierung bei verringertem Bedarf gleichermaßen möglich. Bei Bedarf können Sie einfach in eine höhere Abonnementstufe wechseln.
Leistung und Zuverlässigkeit	Verantwortlich für die Überwachung und Verbesserung der Leistung sowie der Zuverlässigkeit der gesamten Umgebung.	Das CCMS läuft basierend auf leistungsstarken Diensten in globalen Rechenzentren.
Datensicherung und -wiederherstellung	Verantwortlich für die Erstellung und Verwaltung von Backups und bei Bedarf für eine vollständige Disaster-Recovery-Umgebung.	Cloudbasierte CCMS verfügen über regelmäßige, automatisierte Backups und geografisch verteilte Rechenzentren für eine erweiterte Disaster Recovery.
Upgrades und Wartung	Verantwortlich für die Verwaltung von Upgrades für die gesamte Umgebung, einschließlich Netzwerk, Server und Software. Die Ressourcen müssen auch außerhalb der regulären Arbeitszeit eingesetzt werden und zur Gewährleistung minimaler Ausfallzeiten müssen alle Änderungen in Staging-Umgebungen getestet werden.	Regelmäßige Upgrades und Wartung außerhalb der regulären Arbeitszeiten. Alle Änderungen werden vor der Implementierung gründlich getestet und die Ausfallzeiten sind minimal.

Integration in andere Systeme	Individuelle Integrationen zur Ermöglichung der Zusammenarbeit der Systeme innerhalb des Netzwerks bzw. der Netzwerke.	Die Integration erfolgt in der Regel über sichere APIs und vorgefertigte Konnektoren für E-Learning-Systeme, Übersetzungsmanagementsysteme, Wissensdatenbanken und andere Plattformen zur Bereitstellung von Inhalten.
Interne und externe Zusammenarbeit	Für den Zugriff auf das CCMS ist ein Netzwerkzugang erforderlich. Externe Zugriffe erfolgen über ein VPN.	Zugriff auf das System ist mit den etablierten Sicherheitsprotokollen jederzeit von einem beliebigen Ort möglich. Externe Beteiligte können zur Zusammenarbeit an Inhalten eingeladen werden, ohne dass ihnen Zugriff auf etwas anderes als das CCMS gewährt werden muss (explizite Berechtigungen).
Service- und Supportleistungen	Das interne Team ist für die Infrastruktur und den Hardware-/Software-Support verantwortlich. Der CCMS-Anbieter bietet Support für das CCMS und muss möglicherweise vor Ort sein, um Support zu leisten.	Der CCMS-Anbieter leistet den gesamten Support über SLAs und ist vollständig remote.

Sicherheit

Ein CCMS muss sensible Informationen schützen, die Einhaltung gesetzlicher Vorschriften sicherstellen, das Risiko von Datenverlusten mindern und Schutz vor Cyberbedrohungen bieten. Durch die Implementierung robuster Sicherheitsmaßnahmen können Unternehmen ihre wertvollen Informationen wirksam schützen und die potenziellen Folgen von Sicherheitsverletzungen mindern.

Zu den Sicherheitsmaßnahmen gehören:

- Netzwerksicherheit: Einsatz von Firewalls, Einsatz von Systemen zum Erkennen und Verhindern unerlaubter Zugriffe (Intrusion Detection/Prevention Systems, IDS/IPS) sowie Netzwerksegmentierung zum Verhindern unbefugter Zugriffe und zum Mindern potenzieller Bedrohungen.

Darüber hinaus muss der gesamte Netzwerkverkehr zwischen Clients und Servern verschlüsselt werden, um die Daten während der Übertragung zu schützen.
- Berechtigungs- und Zugriffskontrollen: Authentifizierungsmechanismen wie die Multi-Faktor-Authentifizierung (MFA) überprüfen die Identität der Benutzer, bevor sie ihnen Zugriff auf das CCMS gewähren. Auf Rollen und Berechtigungen basierende Berechtigungsrichtlinien steuern den Zugriff der Benutzer auf Funktionen und Ressourcen.
- Datenverschlüsselung: Die Verschlüsselung sensibler Daten, die im CCMS gespeichert sind, schützt diese vor unbefugtem Zugriff oder Manipulation. Robuste Verschlüsselungsalgorithmen gewährleisten die Vertraulichkeit und Integrität gespeicherter Daten.
- Patch-Management: Ein Patch-Management-Verfahren hilft dabei, Sicherheitspatches schnell zu priorisieren und schnellstmöglich zu implementieren, bekannte Schwachstellen zu beheben und das Risiko der Ausnutzung durch Angreifer zu reduzieren.
- Audits und Überwachung: Regelmäßige Sicherheitsaudits und -bewertungen müssen durchgeführt werden, um Schwachstellen zu ermitteln, Risiken zu beurteilen und die Einhaltung von Sicherheitsrichtlinien und -vorschriften zu gewährleisten. Darüber hinaus müssen Überwachungs- und Protokollierungsmechanismen implementiert werden, um Benutzeraktivitäten zu verfolgen, verdächtiges Verhalten zu erkennen und umgehend auf Sicherheitsvorfälle zu reagieren.

Alle oben genannten Maßnahmen sind erforderlich, unabhängig davon, ob das CCMS vor Ort oder in der Cloud gehostet wird. Der Unterschied besteht darin, wer dafür verantwortlich ist, dass diese Sicherheitsmaßnahmen implementiert sind und kontinuierlich verwaltet werden.

Unternehmen mit einem On-Premise Compontent Content Management System sind dafür verantwortlich, dass sich dieses umfassende Maßnahmenpaket zum Schutz des Systems, der Daten und der Infrastruktur in Kraft befindet. Sie benötigen ein Sicherheitsteam, das im Hinblick auf die neuesten Technologien, Verfahren und Zertifizierungen im Zusammenhang mit dem CCMS sowie bezüglich der Hosting-Infrastruktur geschult ist. In den meisten Fällen haben Sie einen Teil dieser Infrastruktur bereits für andere Systeme implementiert. Hier betrachten wir jedoch schwerpunktmäßig, was zur Unterstützung des CCMS erforderlich ist.

Ein cloudbasiertes CCMS übernimmt all diese Sicherheitsmaßnahmen für Sie und investiert in modernste Technologien, wie erweiterte Verschlüsselung, Identitäts- und Zugriffsmanagement sowie Bedrohungserkennungssysteme. Es verfügt über eine kontinuierliche Überwachung und Bedrohungserkennung, um Compliance-Probleme oder

böswillige Bedrohungen zu erkennen sowie Sicherheitsupdates und -patches automatisch zu implementieren.

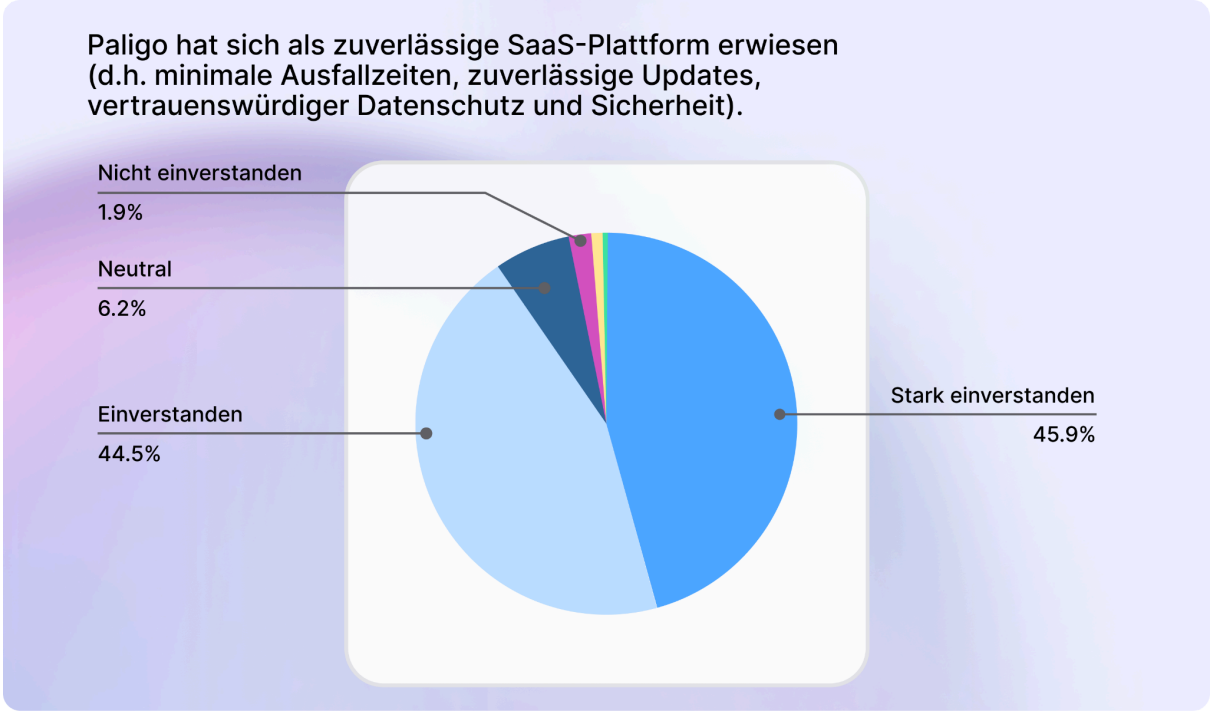
> „Die Cloud birgt sicherlich ihre Risiken, aber SaaS-Umgebungen ermöglichen auch eine schnellere Reaktionszeit bei einem Verstoß sowie eine schnellere Umsetzung von Updates und Patches. Angesichts der heutigen globalen Verteilung von Mitarbeitern stellen die Agilität, Geschwindigkeit und Reichweite von SaaS-Umgebungen greifbare Vorteile dar, die von den meisten Unternehmen nicht verpasst werden sollten."

Quelle: Security Magazine

Einige weitere sicherheitsbezogene Hauptunterschiede zwischen On-Premise- und cloudgehosteten CCMS:

Sicherheitszertifizierung: Als Nachweis der implementierten Sicherheitspraktiken beantragt ein cloudbasiertes CCMS Compliance-Zertifizierungen, z. B. nach ISO 27001, einer internationalen Norm für Informationssicherheits-Managementsysteme.

Auch ein Unternehmen kann diese Sicherheitszertifizierungen beantragen. Allerdings ist es für die Arbeit, die mit der Erlangung – und der kontinuierlichen Beibehaltung – dieser Zertifizierungen verbunden ist, allein verantwortlich. Dies verlangt einen hohen Zeit- und Kostenaufwand.



Source: internal Paligo user survey, March 2024

Datenhoheit: In vielen Ländern ist gesetzlich geregelt, wie Unternehmen in ihrem Land erhobene Daten speichern und verwalten müssen (die DSGVO ist eine EU-Verordnung, die für jedes Unternehmen gilt, das in der EU tätig ist).Diese Regeln und Vorschriften zur Datenhoheit variieren von Land zu Land. Unternehmen, die in mehreren Ländern tätig sind, müssen sicherstellen, dass sie ihre Daten in Übereinstimmung mit den Gesetzen des jeweiligen Landes korrekt verwalten.

Die Datenhoheit kann für ein Unternehmen mit einem On-Premise-CCMS eine Herausforderung darstellen, wenn es nur ein Rechenzentrum hat. Je nach den spezifischen Gesetzen eines Landes kann es erforderlich sein, über Rechenzentren in mehr als einem Land zu verfügen, was kostspielig sein kann. Zusätzlich zur Verwaltung mehrerer Rechenzentren muss das Unternehmen möglicherweise noch CCMS-Lizenzen erwerben oder sich um eine sichere Datenübertragung zwischen den Rechenzentren für deren Verarbeitung kümmern (sofern zulässig).Dies kostet nicht nur Zeit, Ressourcen und Geld, sondern öffnet auch die Tür für Sicherheitsrisiken.

Ein cloudbasiertes CCMS für Kunden in mehreren Ländern ist dafür verantwortlich, sicherzustellen, dass es die Gesetze und Governance-Strukturen jedes dieser Länder einhält. Bei Bedarf wird seine Software in Rechenzentren in den einzelnen Ländern gehostet und sichergestellt, dass alle Sicherheits- und Datenschutzbestimmungen eingehalten werden.

Kostenüberlegungen

Sehen wir uns die Kosten im Zusammenhang mit dem Hosting eines CCMS an.

Eine Installation vor Ort kann eine beträchtliche Anfangsinvestition bedeuten:

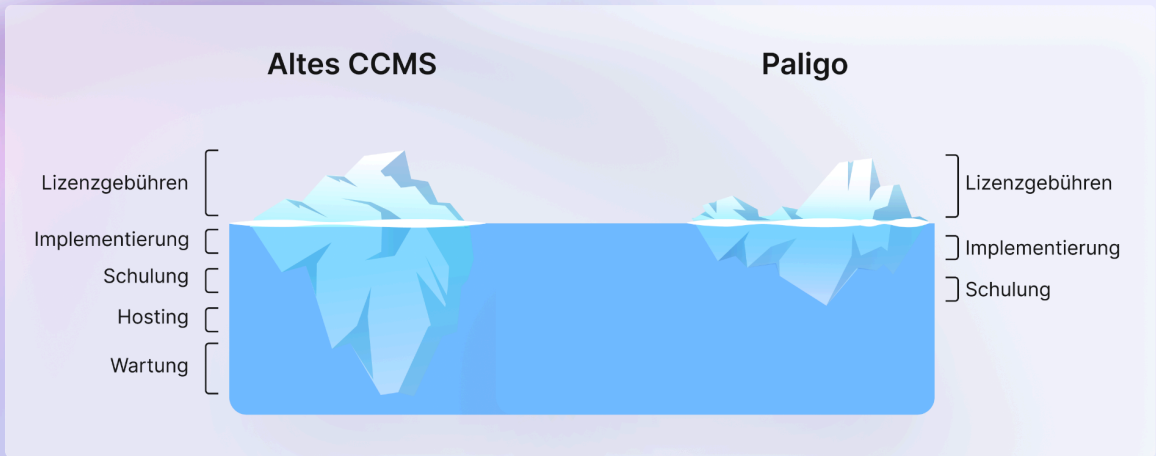
- Server (mehrere, wenn Sie eine Umgebung mit Lastausgleich wünschen) und Backup-Server für den Fall, dass ein Primärserver ausfällt
- Lastausgleichssoftware
- CCMS-Softwarelizenzen
- Backup- und Virenschutzsoftware

- Netzwerkdienste
- Verschlüsselungssoftware

Zusätzlich zur Kapitalinvestition entstehen weitere Kosten in Verbindung mit einer On-Premise-Installation, darunter:

- Ressourcen zur Installation und Verwaltung der Hard- und Software
- Laufende Wartung der Server
- Laufende Wartung für die gesamte beteiligte Software, einschließlich Upgrades oder Patches
- Monatliche Kosten für den Betrieb der Umgebung- Stromversorgung, Kühlsysteme, Sicherheit usw.)
- Ressourcen für die Verwaltung der Sicherheit

Die wirklichen Kosten eines Unternehmens-CCMS



Außerdem verschlechtert sich die Leistung von Servern im Laufe der Zeit oder sie fallen aus. Seien Sie also auf zusätzliche Hardware- und Infrastrukturkosten vorbereitet.

Schauen wir uns nun die Kosten eines cloudbasierten CCMS an. Zunächst einmal fallen in diesem Fall keine Kosten für Vorabinvestitionen an. Diese Kosten werden hier stattdessen in die Monats- oder Jahresbeiträge für das Abonnement des CCMS integriert. Solange Ihre Anforderungen unverändert bleiben, zahlen Sie jährlich denselben Abo-Tarif.

Abonnements werden in der Regel jährlich erneuert, sodass Sie gut kalkulierbare Kosten haben. Und falls Sie Ihr Abonnement nicht verlängern möchten, sind Sie nicht an Kosten für Lizenzen, Hardware oder Infrastruktur gebunden. Stattdessen können Sie Ihre Inhalte aus dem CCMS in eine neue Umgebung migrieren.

Skalierbarkeit

Bei der Ersteinrichtung Ihres CCMS haben Sie eine realistische Einschätzung zum Umfang der Inhalte, die Sie speichern müssen, und zur Erweiterung dieser Inhalte im Laufe der Zeit. Mit diesen Informationen können Sie berechnen, wie groß Ihre Serverumgebung sein muss. Bei einer On-Premise-Umgebung haben Sie die folgenden zwei Möglichkeiten:

- Sie richten die Umgebung für die derzeitigen Inhalte ein und lassen etwas Spielraum für Wachstum. Dies würde Ihre minimale Serverumgebung darstellen.
- Sie richten die Umgebung gemäß den Inhalten ein, die Sie für die kommenden fünf Jahre oder einen längeren Zeitraum erwarten. Eine derart eingerichtete Umgebung erfordert umfangreiche Vorabinvestitionen zur Unterstützung künftiger Erweiterungen. Sie tragen also zusätzliche Kosten für eine Einrichtung, die Sie zwar jetzt noch nicht benötigen, aber Ihrer Einschätzung nach in Zukunft benötigen werden.

Keine dieser Möglichkeiten ist optimal. Wenn Sie die erste Möglichkeit nutzen und plötzlich mit mehr Inhalten konfrontiert werden, als Ihre Umgebung bewältigen kann, müssen Sie die Infrastruktur und Hardware (sowie eventuell auch die CCMSLizenzen) schnell erweitern, um Ihren Anforderungen weiterhin gerecht zu werden. Ein Update der Infrastruktur und Hardware ist nicht einfach. Wenn Sie strengen Compliance- und Regulierungsanforderungen unterliegen, dauert es sogar noch länger, da Sie für eine ordnungsgemäße Implementation und Prüfung dieser Updates sorgen müssen.

Bei einer Entscheidung für die zweite Option geben Sie Geld für eine Umgebung aus, die Sie derzeit noch nicht benötigen, um sich auf eine künftige Situation vorzubereiten. Doch bei knappem Budget sind Ausgaben für nicht benötigte Anschaffungen nie eine gute Entscheidung.

Bei einem cloudbasierten CCMS sieht die Sache ganz anders aus. Ein CCMS mit Hosting in einer Cloud-Umgebung bietet Ihnen sofortige Skalierbarkeit – sozusagen „Scale on Demand“ – zur Erfüllung Ihrer wachsenden Anforderungen. Bei diesem Modell müssen Sie nur für die Dienste bezahlen, die Sie benötigen. Wenn Ihre Anforderungen wachsen und Sie mehr Speicherplatz oder zusätzliche Rechenleistung benötigen, kann die Umgebung Ihres CCMS-Anbieters automatisch skaliert werden, um diese Anforderungen zu erfüllen. Sie müssen nicht auf weitere Server oder Datenspeicher warten; Ihre Umgebung wächst automatisch mit.

Leistung und Zuverlässigkeit

Bei einem internen Hosting Ihres CCMS sind Sie von der Zuverlässigkeit Ihrer lokalen Infrastruktur abhängig. Wenn Sie diese nicht stark oder sicher genug eingerichtet haben, stehen Sie in Zeiten hohen Datenaufkommens vor potenziellen Leistungsproblemen oder riskieren einen Cyber-Hack.

Andererseits läuft ein cloudbasiertes CCMS auf Basis leistungsstarker Dienste in globalen Rechenzentren. Diese Rechenzentren sind im Hinblick auf eine erweiterte Zuverlässigkeit eingerichtet und bieten Service Level Agreements (SLAs), die eine durchgängige Verfügbarkeit gewährleisten.

Der Weltmarkt für Public Cloud wird 2024 voraussichtlich 679 Milliarden US-Dollar erreichen – vor allem durch AWS, Azure und Google. Es ist wichtig, zu wissen, welche Public Cloud ein cloudbasiertes CCMS verwendet.

Quelle: Statista

Datensicherung und Disaster Recovery

Neben der Live-Server-Umgebung benötigen Sie auch individuelle Lösungen für Backup und Disaster Recovery für den Fall, dass in Ihrer Live-Umgebung ein Problem auftritt. Datensicherungen sollten täglich durchgeführt werden; und die Sicherungen sollten auf verschiedenen Servern sowie ggf. in verschiedenen Rechenzentren gespeichert werden.

Eine Disaster-Recovery-Lösung bietet eine duplizierte Umgebung oder eine Reihe von Servern, die online geschaltet werden können, falls in Ihrer Live-Umgebung ein Problem auftritt. Je nach Bedeutung und Sensitivität Ihrer Inhalte muss diese Backup-Umgebung sofort oder innerhalb eines kurzen Zeitfensters online gehen.

Wenn Sie keinen Disaster-Recovery-Plan haben oder Ihre Datensicherungen auf denselben Servern wie Ihre Produktionsumgebung speichern, riskieren Sie, dass Sie Ihre

Inhalte unwiederbringlich verlieren sowie keinen Zugriff auf Ihr CCMS und damit keine Möglichkeit zur Verwaltung Ihrer Inhalte mehr haben.

Bei einem cloudbasierten CCMS müssen Sie sich dagegen keine Sorgen über Backup- und Disaster-Recovery-Umgebungen für Ihre Daten machen. Cloudbasierte CCMS verfügen über regelmäßige, automatisierte Backups und geografisch verteilte Rechenzentren für eine erweiterte Disaster Recovery.

Upgrades und Wartung

Die Wartung Ihrer Serverumgebung ist zeitaufwendig und erfordert qualifizierte Ressourcen. Wenn Sie die CCMSUmgebung offline nehmen müssen, um einen Server zu patchen oder ein Update für das CCMS oder eine andere Support-Software durchzuführen, ist Ihr CCMS für die Dauer der Updates offline.

Bei einem cloudbasierten CCMS erhalten Sie automatische Updates mit minimalen Ausfallzeiten. Neue Funktionen und Erweiterungen können ohne oder nur mit geringfügigen Auswirkungen auf Ihr Unternehmen hinzugefügt werden. Außerdem werden Upgrades vor ihrer Implementierung getestet, damit sie die Produktion nicht beeinträchtigen. Die Ausfallzeiten sind in der Regel minimal und treten außerhalb der regulären Arbeitszeit auf.

Umgang mit Datenschutz- und Compliance-Aspekten in Deutschland

Laut einer aktuellen Studie zu deutschen Unternehmen nutzen 46,5 % die Cloud-Computing-Technologie für ihre Geschäftsprozesse, während 11,1 % dies planen. Weitere 18,2 % der befragten Unternehmen diskutieren noch darüber, ob sie die Technologie einführen oder nicht. *Quelle: ifo Institut*

Laut einer anderen Studie planen 56 % der Unternehmen, in den kommenden fünf Jahren mehr als die Hälfte ihrer IT-Anwendungen in der Cloud zu hosten (derzeit nur 15 %).

> „Das wichtigste Ziel für Unternehmen in Bezug auf ihre Cloud-Aktivitäten besteht darin, die Kosten (64 Prozent) und die CO2-Emissionen (63 Prozent) zu reduzieren. Eine Mehrheit von 57 Prozent möchte zudem IT-Anwendungen in Plattformen und Software-as-a-Service transformieren sowie die IT-Sicherheit erhöhen."

Quelle: Bitkom

Obwohl cloudbasierte Lösungen in Deutschland genutzt werden, gibt es weiterhin Bedenken. Laut Marc Achtelig, *Berater für technische Dokumentation bei indoition*, haben diese Bedenken mehrere Gründe:

> „In Deutschland sind wir häufig der Ansicht, dass ein System dann gut ist, wenn wir es vollständig kontrollieren können. Eine gehostete Lösung können wir aber nicht vollständig kontrollieren. Wir empfinden dies also als großen Nachteil und übersehen die Vorteile, die entstehen, wenn wir das System gar nicht selbst verwalten müssen."
>
> Marc Achtelig, Technical Documentation Consultant at Indoition

Achtelig weist auch auf Bedenken deutscher Unternehmen bezüglich der Datenhoheit hin. Der Begriff Datenhoheit beschreibt, dass erstellte, verarbeitete und gespeicherte Daten und Inhalte den Gesetzen des Landes unterliegen, in dem sie erstellt werden. In Deutschland wird die Art und Weise der Verwaltung und Speicherung von Daten in Unternehmen durch zwei Rechtsvorschriften geregelt: das (*Bundesdatenschutzgesetz (BDSG)*) und die Datenschutz-Grundverordnung der EU (*DSGVO*). Jedes cloudbasierte System muss sicherstellen, dass es diese Vorschriften einhalten kann.

Zusätzlich müssen ggf. unternehmensinterne Compliance-Standards beachtet werden:

> **„In vielen Fällen gelten spezielle Compliance-Anforderungen. Sie können die Einhaltung von Standards erfordern, die ein Unternehmen selbst aufgestellt hat. Die Anforderungen können aber auch die Einhaltung von Standards eines bestimmten Kundenunternehmens erfordern. Lieferanten müssen diese Standards ebenfalls einhalten.“**

Die Antworten auf die Bedenken deutscher Unternehmen hängen letztlich von dem cloudbasierten CCMS ab, das sie betrachten. Hier gehen wir auf fünf Hauptbedenken ein und erklären, welche Antworten das Paligo CCMS und die von Paligo gehostete Umgebung dazu bieten.

Bedenken	Paligo CCMS
Wie sicher ist ein cloudbasiertes CCMS? (Ist es sicher? Ist die Verschlüsselung sicher?)	Paligo nutzt zur Gewährleistung der Sicherheit die etabliertesten Maßnahmen und Plattformen, wobei das Hosting auf Amazon EC2 erfolgt, das die strengsten Sicherheitsstandards erfüllt (SOC1, 2, 3/ SSAE 16, ISO 9001, ISO 27001 und viele weitere). Standardmäßig wird eine 256 Bit SSL-TSL-Verschlüsselung verwendet. Für ausgewählte Pläne sind zusätzliche Sicherheitsstufen verfügbar. Es werden stündlich Backups erstellt, und jedes Backup wird 90 Tage lang gespeichert. Bei einem Vorfall kann aufgrund des Kontrollniveaus dieser Umgebung eine schnelle Wiederherstellung erfolgen. Außerdem verwendet Paligo bei Anmeldungsversuchen eine Zwei-Faktor-Authentifizierung, um die Identität eines Benutzers zu bestätigen.

Entspricht das CCMS der DSGVO? Entspricht es dem BDSG?	Paligo entspricht der DSGVO. Darüber hinaus stellt Paligo in Zusammenarbeit mit seinen Kunden sicher, dass weitere Compliance- und Rechtsvorschriften in Bezug auf die Speicherung und Sicherheit von Inhalten erfüllt werden.
Wo werden meine Inhalte gespeichert?	Paligo verfügt über ein EU-spezifisches Rechenzentrum für die Europäische Union, das bei AWS (in Dublin, Irland) gehostet wird.
Sind wir für immer an das CCMS gebunden?	Paligo bietet zwei Arten von XML-Exporten an, um zu verhindern, dass Sie an einen Anbieter gebunden sind. Sie können Ihre Inhalte im DocBook 5.1 XML-Format oder im Paligo Export Format exportieren, das hauptsächlich zum Verschieben einzelner Inhalte zwischen Paligo-Instanzen bestimmt ist.
Können wir das CCMS an unsere spezifischen Anforderungen anpassen?	Paligo bietet bei Bedarf als Dienstleistung individuell angepasste Datenimporte und Layouts an, außerdem in begrenztem Umfang individuelle Filterattribute.

In praktisch jedem Land haben Unternehmen Bedenken bezüglich der Sicherheit. Es ist jedoch wichtig, zu verstehen, dass cloudbasierte Lösungen keine höheren Risiken als On-Premise-Lösungen bergen. Das Risiko einer Umgebung ist umso höher, je niedriger das Niveau der implementierten Sicherheits- und Datenschutzmaßnahmen ist.

> **„Zwei Drittel (64 Prozent) der Unternehmen, die Cloud-Computing nutzen, geben an, dass sie in den vergangenen zwölf Monaten überhaupt keinen Cyberangriff auf die Cloud-Umgebung hatten. Ein Viertel (26 Prozent) meldete Angriffe, gegen die ihre eigenen Sicherheitsmaßnahmen effektiv waren. Nur 1 Prozent wurde Opfer eines Cyberangriffs auf die Cloud-Umgebung, der zu erheblichen Betriebsunterbrechungen führte.“**

Source: Federal Data Protection Act (BDSG)

Tatsächlich sind cloudbasierte CCMS-Plattformen mit den deutschen Standards und Richtlinien kompatibel. Entscheidend ist, dass die Sicherheit des Systems im vollen Umfang sichergestellt wird sowie dass die länderspezifischen Vorschriften und die Compliance-Regelungen des Unternehmens eingehalten werden. Achten Sie darauf, indem Sie danach fragen.

Integration mit anderen Systemen

Wahrscheinlich müssen Sie andere Systeme (z. B. Übersetzungsmanagement-, Kollaborations- und Kundensupportsysteme) mit Ihrem CCMS integrieren. Bei einer On-Premise-Lösung erfordern diese Integrationen oft individuelle Entwicklungen zur Verbindung der Systeme. Außerdem muss diese Integration verwaltet und aktualisiert werden, wenn sich die Systeme ändern. Zudem müssen sich die Systeme innerhalb derselben Organisation und Infrastruktur befinden, oder sie benötigen einen individuellen Netzwerkzugriff über VPNs oder point-to-point networks.

Ohne die Integration besteht ein hohes Risiko, dass Datensilos entstehen, die zu doppelten Inhalten in verschiedenen System sowie zu veralteten oder ungenauen Inhalten in einem oder mehreren Systemen führen, ohne dass erkennbar ist, in welchem System sich der aktuelle Inhalt befindet.

Solche Probleme gibt es bei einem cloudbasierten CCMS nicht. Die Integration erfolgt in der Regel über sichere APIs und vorgefertigte Konnektoren. Beispielsweise können Sie Ihr CCMS über eine API-Integration mit Ihrer Helpdesk-Wissensdatenbank verbinden. Wenn Sie neue Inhalte in Ihrem CCMS veröffentlichen, werden sie automatisch auch in der Wissensdatenbank veröffentlicht.

Ein cloudbasiertes CCMS ist mit vielen Anwendungen von Drittanbietern kompatibel, unter anderem mit E-Learning-Systemen, Übersetzungsmanagementsystemen, Wissensdatenbanken und anderen Plattformen zur Bereitstellung von Inhalten.

„Die Integrationen sind einfach einzurichten und zu verwenden, und wir nutzen sie für die Veröffentlichung in Zendesk und Amazon S3. Wir haben kürzlich damit begonnen, unser Helpcenter mithilfe der integrierten Paligo Funktion ins Japanische zu übersetzen. Sehr einfach und effizient. Sehr empfehlenswert für alle, die auf eine cloudbasierte Plattform umsteigen möchten.“

Paligo user review on G2

Zusammenarbeit

Bisher haben wir die Unterschiede zwischen einem On-Premise- und einem cloudbasierten CCMS im Hinblick auf Hardware, Software und Infrastruktur behandelt. Die

Nutzung eines cloudbasierten CCMS bietet aber noch weitere Vorteile, insbesondere in den Bereichen Zusammenarbeit und Fernarbeit.

Bei einem cloudbasierten CCMS ist ein Zugriff auf das System jederzeit und von jedem Ort aus möglich. Ob Sie nun im Büro, zu Hause, an einem Partnerstandort oder an einem beliebigen Ort arbeiten wollen: Sie können jederzeit auf das CCMS zugreifen, um Ihre Arbeit zu erledigen.

Wenn Sie mit externen Mitarbeitern zusammenarbeiten, können Sie ihnen einfach Zugriff auf bestimmte Funktionen wie das Überprüfen und Kommentieren von Dokumenten geben. Dabei können Sie auch sicherstellen, dass sie Funktionen wie „Änderungen nachverfolgen“ und Versionskontrolle anwenden.

„Bei unserem letzten Dokumentationstool mussten wir eine Desktop-Anwendung herunterladen, sie mit dem Repository verbinden, das die Support-Website enthielt, und dann die gesamte Website herunterladen, wenn wir etwas bearbeiten wollten. Zur Veröffentlichung der Website musste sie zurück in das Repository verschoben und dann bereitgestellt werden. Paligo hat diesen Prozess vereinfacht, indem alle Schritte in einem Webbrowser ausgeführt werden. Das Entscheidende daran: So können wir die Dokumentation von jedem Gerät mit Internetverbindung aus aktualisieren und bereitstellen, ohne eine ganze Anwendung herunterladen und authentifizieren zu müssen.“

Paligo user review on TrustRadius

So eine einfache Möglichkeit für den Zugriff und die Zusammenarbeit bietet eine On-Premise-Lösung nicht. Bei On-Premise muss jeder, der Zugriff auf das CCMS benötigt, vor Ort sein oder Fernzugriff über ein VPN erhalten (was viele Sicherheits- und Datenschutzbedenken mit sich bringt). Hinzu kommt: Da Ihr CCMS in einem internen Netzwerk gehostet wird, können Sie externen Partnern keinen Zugriff auf die Dokumentation gewähren, um diese zu überprüfen und zu kommentieren.

Service- und Supportleistungen

Obwohl wir dieses Thema zuletzt behandeln, ist es genauso wichtig wie die anderen. Wenn Sie Ihr CCMS lokal hosten, sind Sie für den gesamten Service und Support der Umgebung verantwortlich. Sie haben einen Supportvertrag für das CCMS selbst. Bei

größeren Problemen muss der CCMS-Anbieter aber jemanden direkt zu Ihrem Standort schicken, um Support zu leisten. Der Support vor Ort ist kostspieliger und kann Verzögerungen verursachen, wenn Sie warten müssen, bis die richtige Personen für einen Vor-Ort-Einsatz verfügbar sind.

Service und Support für ein cloudbasiertes CCMS sind hingegen viel einfacher. Der CCMS-Anbieter trägt die volle Verantwortung für die Umgebung und Sie müssen sich um nichts kümmern. Die Support-Mitarbeiter müssen nicht vor Ort sein; sie können aus der Ferne auf Ihr CCMS zugreifen, Ihnen bei der Fehlerbehebung helfen, neue Funktionen einrichten und einfach und schnell auf Fragen reagieren.

IV. Fazit

Die Entscheidung zwischen einer On-Premise- und einer cloudbasierten Lösung für das Component Content Management ist eine strategische Entscheidung, die sich erheblich auf die Effizienz, Sicherheit und Skalierbarkeit eines Unternehmens auswirken kann.

Während in der Vergangenheit traditionelle On-Premise-Lösungen bevorzugt wurden, da sie ein Gefühl der Kontrolle über Sicherheit, Kundenanpassung und Konnektivität bieten, haben sich cloudbasierte Lösungen weiterentwickelt und erfüllen bereits die Anforderungen von Unternehmen mit höchsten Sicherheits- und Compliance-Standards. Cloudbasierte CCMS-Lösungen stellen eine überzeugende Alternative dar: Sie bieten zahlreiche Vorteile, die früher in Bezug auf cloudbasierte Software geäußerte Bedenken überwiegen.

In diesem Whitepaper haben wir dargestellt, warum cloudbasierte CCMS-Lösungen die Zukunft des Component Content Managements sind. Sie bieten eine Kombination aus Sicherheit, Skalierbarkeit, hoher Leistung und guter Zusammenarbeit, mit der Unternehmen in einer zunehmend digitalen Welt erfolgreich bestehen können.

Wir freuen uns, Ihnen bei dieser Gelegenheit zeigen zu können, wie das Paligo CCMS Ihnen die in diesem Whitepaper diskutierten Funktionen zur Verfügung stellt. Die *Sicherheits- und Compliance-Informationen von Paligo finden Sie hier* . Wenn Sie Fragen zu Vertrauenswürdigkeit, Sicherheit und Compliance bei Paligo haben, *finden Sie hier unsere Kontaktinformationen* .

V. Empfehlungen

Wie geht es nun weiter? Investieren Sie in ein On-Premise- oder in ein cloudbasiertes CCMS? Hierzu müssen Sie eine fundierte Entscheidung treffen, denn auf diese Frage gibt keine richtige Antwort, sondern nur eine Antwort, die für Ihr eigenes Unternehmen die richtige ist.

Nehmen Sie sich die Zeit und Nehmen Sie sich Zeit und skizzieren Sie Ihre Anforderungen in folgenden Bereichen:

- Welche Funktionen benötigen Sie in einem CCMS?
- Mit welchen Systemen müssen Sie es integrieren, und wo befinden sich diese?
- Benötigen Sie Fernzugriff für Mitarbeiter oder Partner?
- Wie viel Speicher- und Rechenleistung benötigen Sie jetzt und in naher Zukunft? Ist das Wachstum beträchtlich oder noch unbekannt?
- Verfügen Sie über ein bestehendes Rechenzentrum und eine Infrastruktur, in der Sie ein CCMS platzieren können?
- Verfügen Sie über Ressourcen mit den richtigen Fähigkeiten und der richtigen Verfügbarkeit, um eine On-Premise-Lösung zu verwalten?
- Verfügen Sie das nötige Budget, um eine lokale Umgebung einzurichten und zu pflegen? Und wenn ja, nutzen Sie Ihr Budget und Ihre Ressourcen damit am besten?

Berücksichtigen Sie die langfristigen Vorzüge und die strategischen Vorteile eines cloudbasierten CCMS gegenüber einer On-Premise-Lösung!

VI. Über Paligo

Paligo ist ein cloudbasiertes Componenten Content Management System (CCMS) mit einer leistungsstarken Single-Sourcing-Möglichkeit zur Mehrfachnutzung von Inhalten beim Erstellen Technischer Dokumentation, zum Erstellen von Schulungsinhalten, für die Dokumentation von Geschäftsprozessen sowie für ein effizientes Wissensmanagement.

Erfahren Sie noch heute mehr über Paligo