LESSIE netzwerk

Bausteine der Digitalisierung:

Cloudspeicher für die Services von Unternehmen nutzen

Autoren: Dr. Kyrill Meyer, Dr. Jörg Härtwig, Steffen Hahn

Whitepaper Version 1.0

Inhalt

Dieses Whitepaper dokumentiert ein Anwendungsszenario im Unternehmenskontext und wurde mit Unterstützung des LESSIE-Netzwerkes erarbeitet.

LESSIE (Leipziger Smart Service Engineering) unterstützt als Initiative und Netzwerk im Raum Mitteldeutschland/Sachsen die **Zusammenarbeit** und **Vernetzung** von regionalen Akteuren und die **Entwicklung intelligenter Dienstleistungen**.

LESSIE ist offen für Unternehmen aller Branchen und Bereiche, die sich im Zuge der Digitalisierung weiterentwickeln und/oder dazu Erfahrungen und Kompetenzen weitergeben möchten. Die Mitglieder und Partner arbeiten gemeinsam daran, **Innovationspotenziale** in Produkten, Prozessen und Geschäftsmodellen zu finden und mit digitalen Technologien in **Smart Services** zu transformieren.

Interessiert am Netzwerk? Kontaktieren Sie LESSIE unter
https://lessie.network/kontakt/

„Der reibungslose digitale Informationsaustausch wird für die Services der LIPSIA Automation GmbH immer wichtiger. Gemeinsam mit den Partnern des LESSIE-Netzwerkes konnten wir im Bereich Cloudspeicher die Digitalisierung in unserem Unternehmen bedeutend weiterentwickeln."

Steffen Hahn, Geschäftsführer
LIPSIA Automation GmbH

Die LIPSIA Automation GmbH wurde 1995 in Leipzig als ein Maschinenbauunternehmen gegründet und hat sich auf maßgeschneiderte Handling- und Verpackungslösungen spezialisiert.

www.lipsia.com

Kollaboration ist bei modernen Dienstleistungsangeboten von Unternehmen ein wichtiger Faktor. Die Zusammenarbeit mit Lieferanten, Dienstleistern, Kunden und Mitarbeitenden benötigt Mittel und Wege für den Austausch sowie Synchronisation über die verschiedensten Informationskanäle hinweg.

Hilfreich sind dabei Cloudspeicher mit ihren unterschiedlichen Funktionen. Überlegungen und Möglichkeiten für die Einrichtung und Nutzung im Unternehmenskontext werden anhand eines Unternehmensbeispiels der LIPSIA Automation GmbH in Brandis nachfolgend vorgestellt.

Cloudspeicher im Unternehmenskontext

In der Informations- und Wissensgesellschaft ist die Arbeit mit aufbereiteten Daten der entscheidende Produktionsfaktor. Früher war der zentrale Unternehmensserver im Intranet hierfür wesentlich und erfasste alle relevanten Informationen auf einem System des jeweiligen Betriebes. Im Vergleich dazu gibt es heute eine Vielzahl von Datenquellen, Analysesystemen und Endgeräten, die für eine kollaborative Arbeit, auch über die Firmengrenze hinweg, synchronisiert werden müssen und Zugriff auf einen gemeinsamen Datenbestand bieten. Im Kern geht es dabei darum, die notwendigen Informationen in geeigneter Form, zur richtigen Zeit, an genau der Stelle zur Verfügung zu stellen, wo sie benötigt werden. Sei es, um Mitarbeitenden die Arbeit im Homeoffice zu ermöglichen, die Kundschaft in Wertschöpfungsprozesse, wie z.B. die Produktentwicklung zu integrieren oder Prozessabläufe weiterzuentwickeln und neu zu erfinden.

Für diese Aufgaben eignen sich Cloudspeicher, die moderne Kommunikations- und Kollaborationsformen unterstützen. In einer Cloud werden alle relevanten Daten auf einem Internet-Server zentral gespeichert. Diese können über das Internet von unterschiedlichen Nutzenden prinzipiell von überall, jederzeit und mit verschiedenen Endgeräten abgerufen, bearbeitet und synchronisiert werden.

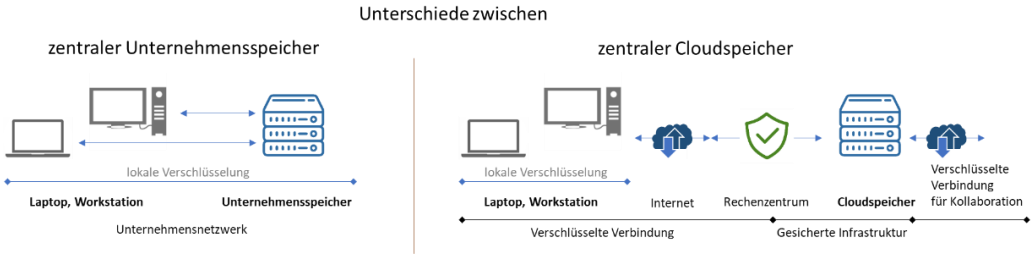

Abbildung 1 - Unterschied zwischen Unternehmensdatenspeicher und Cloudspeicher

Mit diesem technischen Potenzial ist für Unternehmen die Herausforderung verbunden, eine passfähige Integration in die betrieblichen Abläufe zu erarbeiten. Entscheidend ist ein Verständnis für die notwendigen Abläufe und Datenflüsse. Dafür bieten die existierenden Cloudlösungen in der Regel weitreichende Möglichkeiten zur Steuerung und Kontrolle und ermöglichen z.B. Zugriffsbeschränkungen, Verschlüsselung oder Freigabeprozesse. Die Einschätzung der Vertraulichkeit der geteilten Daten oder die Verzahnung von Zugriffsrechten mit dem Unternehmensorganigramm, bzw. vertraglichen Vereinbarungen, sind aber quasi als Voraussetzung für eine sinnvolle Nutzung gesondert zu erfassen und geeignet abzubilden. Dies geschieht idealerweise bereits im Rahmen einer Digitalisierungsstrategie. Dadurch lassen sich Anforderungen konkretisieren, z.B. dass eine Rechteverwaltung auch auf Datei-Ebene möglich notwendig ist oder die Cloud mit dem im Unternehmen möglicherweise verwendeten Single-Sign-On[1] Verfahren kompatibel sein muss. Ebenfalls relevant können in diesem Zusammenhang die Fragen nach der Integration der Daten in unterschiedliche Programme sein: reicht die Möglichkeit, Dateien mit Office-Programmen öffnen zu können, oder sollen diese ebenfalls mit dem Kalender und einer Projektmanagement-Software interagieren? Sollen Mediadateien in der Cloud abspielbar sein? Gibt es Unternehmenspläne, in Zukunft vermehrt auf digitale Videokonferenzen abzustellen? Auch hierfür sind bereits cloudbasierte und integrierbare Lösungen verfügbar. Und nicht zuletzt ist auch die Frage zu stellen, wie komfortabel die eingesetzte Lösung zu bedienen sein soll oder sich in Bezug auf Sprache und

[1] Single Sign-on (SSO) ermöglicht, dass ein Benutzer sich einmalig an einem Gerät anmeldet und danach auf verschiedenste Dienste zugreifen kann, ohne sich an den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen.

Layout an die Vorgaben und Vorstellungen des nutzenden Unternehmens anpassen lässt.

Die Formulierung der eigenen Anforderungen, unter Einbezug der Erfordernisse an die Datenkontrolle, ist die Grundlage für die Wahl einer Cloudlösung. Hinzu kommt ein Wissen über die vorhandenen Cloudanbieter und ihre Leistungsangebote und Möglichkeiten.

Sicherheit und Datenschutz in der Cloud

Verschiedene kommerzielle Anbieter bieten Cloudspeicherlösungen „as a Service" an. Oft besteht die Möglichkeit der Nutzung einer kostenfreien Variante mit begrenztem Speicherplatz, welcher sich kostenpflichtig erweitern lässt. Die Nutzung eines solchen Dienstes scheint zunächst schnell und einfach. Die große Herausforderung für Unternehmen hinsichtlich der Nutzung solcher Lösungen, ist die Möglichkeit der Bewertung des Datenschutzes und der Datensicherheit. Schließlich muss man dem Anbieter vertrauen, dass er mit den Daten verantwortlich umgeht und sie an einem sicheren Standort ohne Zugriffsmöglichkeit für Dritte speichert. Eine große Anzahl der bekannten Cloud-Speicher-Anbieter hat ihren Firmensitz in den USA, betreibt die Server für den Datenaustausch außerhalb der EU und unterliegt damit dem dortigen Rechtsrahmen. Im Ergebnis können z. B. US-amerikanische Geheimdienste die Herausgabe von Daten bei den dort ansässigen Anbietern (und eingeschlossen damit auch die Einsicht auf die gespeicherten Informationen) einfordern[2], was im Konflikt zu deutschen bzw. europäischen Rechtsvorschriften stehen kann. Für Unternehmen kann hier eine Alternative darin bestehen, auf Anbieter zurückzugreifen, die dem EU-Recht und dem EU-Datenschutz unterliegen.

Ein weiterer zu beachtender Aspekt ist die Weitergabe bzw. der Umgang mit den hinterlegten Daten. Cloud-Anbieter verlangen für die Bereitstellung des Zugangs normalerweise Konto- und Anmeldedaten wie Name, Adresse, E-Mail, Telefonnummer und Zahlungsinformationen. Diese Daten werden gespeichert, verwendet und – je nach Anbieter und Datenschutzerklärung – auch weitergegeben.

Und was ist mit den in die Cloud hochgeladenen Daten? In den Nutzungsbedingungen der verschiedenen Anbieter wird in der Regel die Wahrung des Datenschutzes besonders betont. Gleichzeitig sind die Regelungen dazu häufig umfangreich, schwer verständlich und im Detail unkonkret oder so formuliert, dass den Anbietern weitgehende Freiheiten im Umgang mit den gespeicherten Daten eingeräumt werden. Unabhängige Analysen zeigen auf, dass die hochgeladenen Inhalte häufig nicht nur einfach gespeichert werden, sondern den Nutzenden auch das Kopieren, Verschieben, Modifizieren, Auswerten, Loggen oder eine andersweitige Nutzung gestattet[3].

[2] Beispielsweise erlaubt der im Nachgang der Terroranschläge am 11. September 2001 in den USA als Bundesgesetz erlassene PATRIOT Act US-Behörden wie dem FBI, der NSA oder der CIA den Zugriff ohne richterliche Anordnung auf die Server von US-Unternehmen und ausländischen Tochterfirmen.

[3] vgl. z.B. Informationen des Heise Verlags unter https://www.heise.de/download/blog/Cloud-Anbieter-Wie-steht-es-um-den-Datenschutz-3658164, zuletzt abgerufen am 11.06.2020

Für Unternehmen ergibt sich die Frage, ob die in einem Cloud-Speicher abgelegten Daten besonders schutzwürdig sind. Ist dies bei Marketingunterlagen vielleicht nicht immer der Fall, sieht es bei sensiblen Firmeninformation, wie z. B. Konstruktionsplänen sicher anders aus. Der Schutz der Daten unterliegt, neben der firmenindividuellen Einstufung, auch stets den rechtlichen Erfordernissen. Besonders relevant ist der Umgang mit personenbezogenen Daten, die durch die Personalabteilung oder den Vertrieb regelmäßig gespeichert und verarbeitet werden. Bei Nutzung eines Cloudspeichers kann es vorkommen, dass auch dort personenbezogene Daten hinterlegt werden. Dann müssen europäische Unternehmen beim Speichern und Verarbeiten von personenbezogenen Daten zwingend die Anforderungen aus der Datenschutzgrundverordnung (DSGVO) beachten. Weiterführende Anforderungen für den Datenschutz ergeben sich in bestimmten Bereichen wie dem Umgang mit Sozialdaten und aus den Anforderungen an den ordentlichen Kaufmann. Nur wenn der Cloudspeicher die rechtlichen Vorgaben in geeigneter Form technisch abbilden kann, ist der ordnungsgemäße Einsatz für Unternehmen überhaupt erst möglich.

Und wie sieht es mit den sonstigen Sicherheitsvorkehrungen der Anbieter von Cloud-Lösungen aus? Auch hier lohnt eine genaue Betrachtung der verschiedenen Anbieter. Wenngleich grundsätzlich viele technische Aspekte wie eine Sicherung der Rechenzentren, verschlüsselte Datenübertragung und -speicherung sowie die Arbeit mit geeignetem Personal als weitgehend gegeben vorausgesetzt werden, werden immer wieder Sicherheitspannen großer kommerzieller Anbieter bekannt. Dann werden auch Unternehmens- und Kundendaten kompromittiert. Dies liegt vor allem auch daran, dass Anbieter, bei denen viele Kunden ihre Daten hinterlegen, ein lohnendes Ziel für Hacker darstellen. Aus der Historie der Vorfälle und der Reaktion der betroffenen Unternehmen in solchen Fällen lässt sich eine Auswahl eines geeigneten Anbieters ebenfalls motivieren.

Als Alternative zur Nutzung eines kommerziellen Anbieters ist der Aufbau einer eigenen Infrastruktur in Verantwortung des jeweiligen Unternehmens möglich. Diese als private Cloud bezeichneten Lösungen bieten hinsichtlich des Datenschutzes und der Datensicherheit die maximale Kontrolle. Es ist klar dokumentierbar, an welcher Stelle sensible Dokumente gespeichert werden und wer darauf Zugriff hat. Aus datenschutzrechtlicher Sicht wird die Gefahr von Verstößen minimiert. Die nötigen Hardware-Ressourcen lassen sich auch in einem solchem Falle bei einem Dienstleister anmieten. Im Vergleich zu einem Speicherdienst entsteht aber ein größerer Wartungsaufwand: Sicherheits-Aktualisierungen für die eingesetzten Betriebssysteme und Software sowie die korrekte Konfiguration müssen in geeigneter Form in Eigenregie realisiert werden.

Will ein Unternehmen also einen Cloudspeicher nutzen, steht es vor einer Auswahlentscheidung und es müssen die verschiedenen Aspekte gegeneinander abgewogen weden (vgl. Tabelle 1).

	Public Cloud	**Private Cloud**	
		Eigener Server	**Gemieteter Server**
Investitions-kosten	Gering	Hoch	Gering
Regelmäßige Kosten	Häufig Pay-per-Use und kostengünstig; Kosten sollten aber regelmäßig überwacht werden	Kosten für Betrieb, Wartung und Erneuerung der Server; evtl. Kosten für die Software	Pauschalbetrag für die Hardware; evtl. Kosten für die Software
Erforderliches IT-Know-How	Gering	Hoch	Geringes Know-How für die Server, evtl. hohes Know-How für Software
Skalierbarkeit	Ja	Ja	Ja
Kosten für Skalierbarkeit	Erhöhte regelmäßige Kosten	Hohe Investitionskosten und erhöhte regelmäßige Kosten	Erhöhte regelmäßige Kosten
Einstiegs-hürden (Kosten und Know-How)	Gering	Hoch	Mittelhoch
Möglichkeiten der Individuali-sierung	Häufig gering, weil Cloudspeicher für viele Anwendungsszenarien ausgelegt	Hoch	Hoch
Daten-sicherheit serverseitig	In der Regel hoch, Sicherheitsprobleme bei verschiedenen Anbietern bekannt	Je nach Konfiguration, hoher Datenschutz möglich	Hoch
Aspekte Datenschutz	Hängt u.a. ab von 1. Serverstandort: USA z.B. geringer Datenschutz, 2. Klauseln in den AGBs	Je nach Konzept, hoher Datenschutz möglich	Je nach Konzept, hoher Datenschutz möglich
Back-Up Konzept	Häufig vorhanden	Muss selbst erstellt werden	Muss selbst erstellt werden

Tabelle 1 - Public vs. Private Cloud

Praxisbeispiel: Erarbeitung und Umsetzung eines Cloudspeicherkonzeptes

Im Rahmen der Aktivitäten des LESSIE-Netzwerkes, mit Unterstützung der Netzwerkpartner, wurde für die LIPSIA Automation GmbH (LIPSIA) eine Cloudspeicherlösung evaluiert und implementiert.

Die Firma LIPSIA wurde 1995 in Leipzig als ein Maschinenbauunternehmen gegründet und hat sich auf maßgeschneiderte Handling- und Verpackungslösungen in der Lebensmittelindustrie spezialisiert. Sie konzipiert und realisiert für ihre Kundschaft im In- und Ausland mittel- und großformatige Fördertechnik. Die jeweilige Lösung wird dabei im Rahmen eines Projektes erarbeitet. In die einzelnen Projekte sind neben den verschiedenen Fachabteilungen der LIPSIA, wie der Konstruktionsabteilung oder der Mechatronikabteilung, auch weitere externe Dienstleister und natürlich der Kundschaft selbst eingebunden. Häufig ist es notwendig, zwischen den Beteiligten Daten wie z.B. Konstruktionspläne oder Steuerungscode auszutauschen. Den Bedarf nach einem Austausch der projektbezogenen Informationen adressierend, hat die Firma LIPISA bereits vor einiger Zeit eine Cloudspeicherlösung als Service eines Unternehmens eingekauft. Eine Bewertung dieser in Teilen des Unternehmens eingesetzten Lösung sowie die Anforderungen der LIPSIA an einen Cloudspeicher im Sinne eines Kriterienkataloges, bildeten die Grundlage für die weitere Arbeit (Auszug in Tabelle 2).

Anforderung	**Bewertung bisherige Lösung / Bedarf**
• Datenaustausch und Synchronisierung zwischen verschiedenen internen und externen Nutzenden notwendig	• Bisherige Lösung hat eingeschränkte Nutzerverwaltung und Rechtevergabe • Feingranulare Zugriffsverwaltung wird benötigt
• Ortsunabhängiger Zugriff mit unterschiedlichen Endgeräten notwendig	• Wird durch bisherige Lösung gut ermöglicht, sollte in gleicher Weise weiterhin möglich sein
• Datenschutz muss eingehalten werden	• Bisheriger Anbieter ist ein amerikanisches Unternehmen, Speicherung der Daten außerhalb Europas ist problematisch • Unbestimmte Formulierungen in den Nutzungsbedingungen räumen dem Anbieter großen Spielraum im Umgang mit den Daten ein, dies ist ungünstig • Klarer Bedarf für eine datenschutzkonforme Lösung wird gesehen
• Datensicherheit muss gewährleistet sein	• Mehre Datensicherheitsvorfälle beim bisherigen Anbieter sind bekannt • Keine verschlüsselte Speicherung bzw. Transparenz bzgl. der Datensicherheit beim bisherigen Anbieter • Datensicherheit soll stärker kontrollierbar sein

• Kostentransparenz	• Monatsgebühr beim bisherigen Anbieter • Laufende Kosten und Initialkosten sollten transparent sein
• Look & Feel / Corporate Identity	• Benutzbarkeit beim bisherigen Anbieter in Ordnung, keine Anpassung an Corporate Identity möglich • Es besteht der Wunsch nach einer Cloud-Lösung im Corporate Design der LIPSIA

Tabelle 2 - Bewertung bisherige Lösung / Anforderungserhebung (Auszug)

Im Ergebnis der Bewertung des bisherigen Anbieters und möglicher Alternativen wurde durch die LIPISA die Entscheidung getroffen, in Zukunft eine private Cloud in Eigenverantwortung für das Unternehmen zu betreiben.

Als Entscheidungsgrundlage für die Wahl einer geeigneten IT-Infrastruktur für die private Cloud wurden zunächst die Anzahl der pro Jahr durchzuführenden Projekte und die dabei anfallende Datenmenge abgeschätzt. Auf dieser Basis fiel die Entscheidung, einen Server in einem deutschen Rechenzentrum mit geeigneter Kapazität anzumieten. Als Vorteile dieser Variante werden gesehen:

- die genaue Kenntnis des Serverstandortes und der daraus resultierende Rechtsrahmen;
- die Kalkulierbarkeit der Kosten;
- die Möglichkeit, Serverkapazitäten unkompliziert den steigenden und sinkenden Bedarfen anpassen zu können;
- vollständige administrative Kontrolle über den Server (für Betriebssystem und eingesetzte Software).

Die Anforderungen an die Cloudsoftware ergaben sich u.a. aus der projektorientierten Arbeitsweise. Um eigene Beschäftigte, externe Dienstleister und die Kundschaft in die jeweiligen Projekte einbinden zu können, wird ein Rechtemanagement für eine feingranulare Vergabe von Lese- und Schreibrechten benötigt. Um allen Projektbeteiligten immer einen Zugriff auf den aktuellen Datenbestand zu ermöglichen, wurde als weitere Anforderung die Möglichkeit der automatischen Synchronisation der Daten für die Endgeräte der Nutzenden benannt. Die Übertragung soll dabei durch geeignete Sicherheitsmechanismen, wie z.B. eine verschlüsselte Datenübertragung nach aktuellen Standards, möglich sein. Auch ein browserbasierter Zugriff auf die Daten der Cloud soll einfach durchzuführen sein. Dabei bestand der Wunsch, die Cloud durch das Einfügen des Firmenlogos und den entsprechenden Farben an das Corporate Design des Unternehmens anzupassen. Im Ergebnis wurde die OpenSource-Lösung Nextcloud zur Umsetzung der privaten Cloud bei der LIPSIA, mit der Erweiterung „GroupFolders" ausgewählt, installiert und an das Corporate Design der Firma angepasst.

Um die Cloud für die Projektarbeit nutzen zu können, folgten weitere Arbeitsschritte. Zunächst wurde dafür eine Ordnerstruktur festgelegt, die als

Basis für die zukünftigen Projekte dienen soll. Zusammenhängend damit, wurde eine Zugriffsmatrix erarbeitet, die den Zugriff sowie die Verantwortlichkeiten für Freigabeprozesse fixiert. Hierzu wurde mit einem Testprojekt gearbeitet. Im Verlauf des Testprojektes konnten die Anforderungen überarbeitet und geprüft werden.

Essentiell für die Arbeit bei der LIPSIA ist die Synchronisation zwischen dem Firmen-Intranet und der Cloud. Hierzu wurden begleitend und unter Nutzung der für Nextcloud verfügbaren Desktop- und Mobil-Clients ein Synchronisationskonzept entwickelt und durch die IT-Administration sowohl auf den relevanten zentralen IT-Systemen als auch auf den Clientgeräten eingeführt. Dabei erfolgte auch eine Einbindung der Cloudlösung in das bestehende Backupkonzept, um einem Datenverlust vorzubeugen.

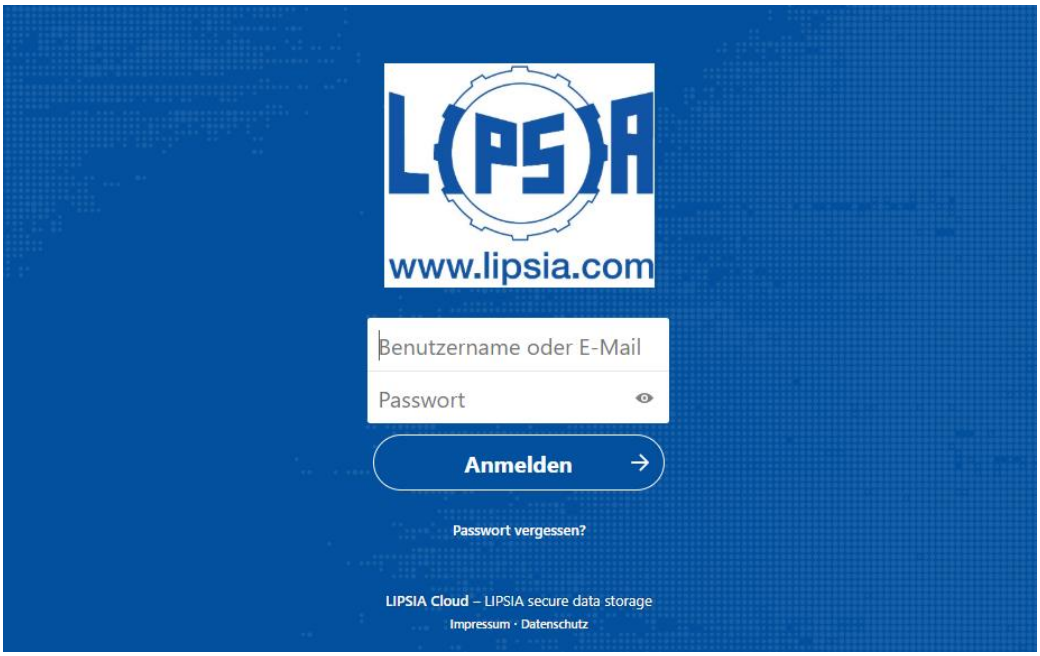

Abbildung 2 – Login der LIPSIA-Cloud

Begleitend zum Testprojekt erfolgt eine Einführung der involvierten Beschäftigten in die Nutzung der Cloudspeicher-Funktionalität. Ebenso erfolgte eine Administratorenschulung und die schriftliche Dokumentation der verschiedenen Aufgaben und Arbeitsschritte.

Zusammenfassung

Im Ergebnis betreibt die Firma LIPSIA eine Cloudspeicherlösung in eigener Verantwortung und Kontrolle mit geringem Aufwand und hohem Nutzen. Mit der Wahl für eine OpenSource-Lösung kann LIPSIA darauf vertrauen, dass die Software frei von Schadware ist und festgestellte, sicherheitsrelevante Schwachstellen in der Regel durch die weltweite Entwicklercommunity schnell beseitigt werden. Kosten für Lizenzen entfallen und der Datenschutz kann durch die eigene Betreuung der Lösung in besonderer Weise sichergestellt werden.

Die Kommunikation zwischen den Endgeräten und der Cloud erfolgt verschlüsselt (End-To-End). Mit der erarbeiteten Zugriffsmatrix und der festgelegten Ordnerstruktur ist sichergestellt, dass die relevanten Akteure im Projekt zuverlässig Informationen in Form von Daten austauschen können. Durch die Synchronisation der Daten greifen alle Nutzergruppen auf die aktuellen Datenbestände zu. Mit der Entscheidung für die Verwendung einer Cloud für das Wissensmanagement und die Zusammenarbeit mit unterschiedlichen Projektpartnern, hat LIPSIA einen Baustein für die Digitalisierung des Unternehmens umgesetzt. Als innovatives Unternehmen plant sie auf dieser Grundlage weiterführende Digitalisierungsschritte und Dienstleistungsangebote mit der Cloud zu verzahnen.

Haben Sie Fragen zur LESSIE-Methode oder wollen Sie Teil des Netzwerks werden, dann kontaktieren Sie uns unter: info@lessie.network oder über das Kontaktformular auf unserer Website https://lessie.network.

LESSIE netzwerk

SACHSEN

Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes

Aus Gründen der besseren Lesbarkeit wird im Text auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.