# Digitale Transformation und Privatsphäre

**Die digitale Transformation** revolutioniert Geschäftsprozesse und Privatleben gleichermaßen. Datensicherheit und Datenhoheit sind zunehmend gefährdet und eine wachsende Zahl von Nutzern verlangt nach verlässlichen Lösungen. Tatsächlich transparente Lösungen scheinen rar.

Die Digitalisierung von Geschäftsprozessen bietet entscheidende Wettbewerbsvorteile und kaum ein Unternehmen kann sich der Nutzung softwarebasierter Dienste entziehen, ohne Gefahr zu laufen, den Anschluss an den nationalen und internationalen Markt zu verlieren. Egal ob durch Cloud, Software-as-a-Service oder andere Angebote entwickelt sich eine zunehmende Auslagerung von Daten und Dienstleistungen an externe Serviceanbieter und fremdgemanagte IT-Infrastruktur.

Genau hier beginnt das Problemfeld in Bezug auf die Hoheit und Vertraulichkeit/Privatsphäre der Daten. Da die datenverarbeitende Infrastruktur der vollständigen Kontrolle eines Drittanbieters unterliegt, hat der Anbieter des Dienstes die vollständige Kontrolle über alle verbreiteten Daten.

Selbst die oft gepriesene Verschlüsselung der Information schafft keinen Vorteil, da letztendlich der Provider in Besitz der Schlüssel oder zumindest des „Master Key“ ist.

Ein kurzer Vergleich mit der analogen „Vergangenheit“ kann dies veranschaulichen: Haben Sie vertrauliche Dokumente und Ordner in Ihrem Büro eingeschlossen, zu dem nur Sie den Schlüssel haben, so können Sie sicher sein, dass – solange Sie den Schlüssel nicht in Hände Dritter geben – Ihre Daten sicher sind. Bewahren Sie hinge-

**Selbst die oft gepriesene Verschlüsselung der Information schafft keinen Vorteil, da letztendlich der Provider in Besitz der Schlüssel oder zumindest des „Master Key“ ist.**

gen diese Dokumente im Archiv Ihrer Firma auf, so haben potenziell alle Zugriff, die in Besitz des Archivschlüssels sind. Dies wäre vergleichbar mit der haus-

internen IT, deren Administrator zumindest potenziell Zugang zu allen ihren Daten hat.

Im Beispiel eines Cloud-Services stehen Ihre vertraulichen Dokumente und Ordner in einem Raum, den ein „fremder" Dritter verwaltet. Das bedeutet, dieser Dritte – der Provider – hat vollständigen Zugriff auf alle dort verwahrten Daten. Das ist die aktuelle Situation bei herkömmlichen Cloud-Diensten, unabhängig davon, ob die Ablage der Daten dort (durch den Anbieter) verschlüsselt oder unverschlüsselt erfolgt.

### Speicher-Sicherheit versus Daten-Sicherheit

Zu oft wird bei Angeboten von providerbasierten Angeboten pauschal Sicherheit bzw. Security propagiert, ohne zu differenzieren, welche Sicherheit genau gemeint ist. Sicherheit von Daten ist zu unterteilen in

- das Minimieren des Risikos Daten zu verlieren (Speichersicherheit) und
- der Absicherung der Daten vor dem Zugriff unberechtigter Dritter (Datensicherheit).

Diese beiden Aspekte von Sicherheit haben grundsätzlich unterschiedliche Implikationen auf die Datenhaltung und das Datenmanagement.

Die Sicherheit vor Verlust der Daten lässt sich durch konse-

Fotos: © iStockphoto, Unternehmen

quente Backups bzw. Vervielfältigung mit Verteilung auf unterschiedliche ggf. auch örtlich getrennte IT-Infrastrukturen gewährleisten.

Der ausschließlich berechtigte Zugriff und damit die Datensicherheit werden durch eine effektive Zugriffskontrolle auf den Datenspeicher sichergestellt.

Es wird deutlich, dass die beiden Sicherheitsbedürfnisse gegenläufig sind. Auf der einen Seite erhöhen mehrere Speicherorte die Speichersicherheit, zum anderen erhöhen genau diese den Aufwand der Zugriffskontrolle. Faktisch sind heutzutage die Datensicherheit und damit die Datenhoheit die zentralen Herausforderungen.

## Zunehmende Abhängigkeit von IT-Infrastruktur und deren Anbieter

Die Bereitstellung digitaler Services stellt nicht zuletzt aufgrund der weltweiten Vernetzung über das Internet an Hardware und Software hohe Anforderungen. Diese Komplexität führt zu professionell outgesourcten Angeboten mit umfangreicher Nutzung externer IT-Infrastruktur. Allein beim Versenden einer E-Mail sind eine Vielzahl an Servern, Routern und Leitungen beteiligt, bis die Nachricht ihren Empfänger erreicht hat.

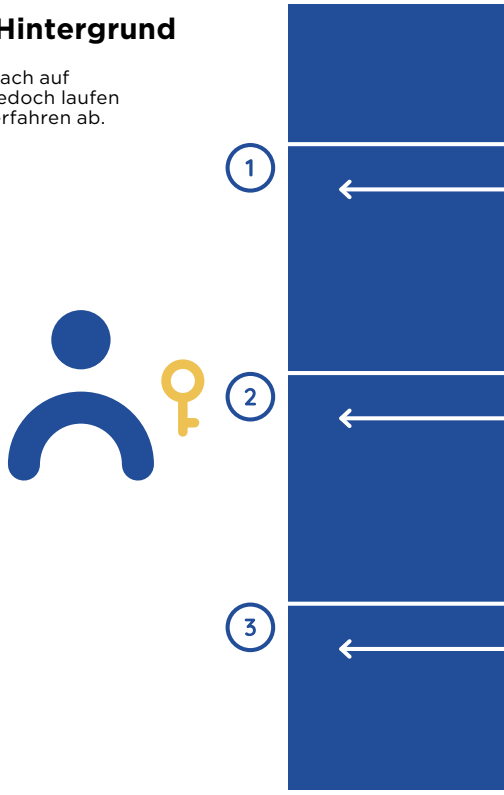
Diese IT-Infrastruktur ist zwangsläufig unter der Kontrolle von Dritten was – um beim Beispiel der E-Mail zu bleiben – zu einem vollständigen Verlust der Datenhoheit nach dem Versenden der (unverschlüsselten) Nachricht führt. Gleiches gilt für Up- oder Download von Daten bei Cloud-Services. Die IT-Infrastruktur wird zu einem zunehmenden Unsicherheitsfaktor im modernen Datenmanagement.

Aus gutem Grund hat die ENISA (die European Network Information Security Agency) neun „high probability high impact risks“ für cloudbasierte Services definiert. Im Folgenden sollen vier dieser Risiken kurz ausgeführt werden:

**Mühelos für Dich, komplexe Technologie im Hintergrund**

Mit olmogo ist es für den Nutzer ganz einfach auf seine Daten zuzugreifen. Im Hintergrund jedoch laufen unmerklich komplexe Operationen und Verfahren ab.

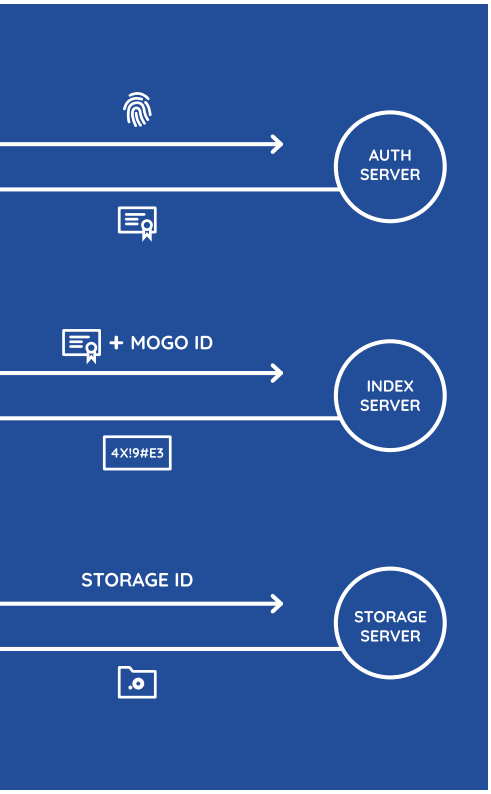
1. Nach der Authentifizierung bescheinigen die olmogo Server die Identität des Nutzers.
2. Für noch größere Sicherheit speichert olmogo Daten nicht nur verschlüsselt, sondern verteilt sie auch – wie ein Puzzle – über mehrere Server hinweg. Die Server liefern die Codes für den Zugriff auf die Speicherorte, in denen die gewünschten Daten liegen.
3. Von diesen Servern werden mithilfe der Zugriffscodes die gewünschten Daten verschlüsselt abgerufen und sicher an das berechtigte Endgerät des Nutzers geliefert. Das Endgerät entschlüsselt die Daten.




Quelle: Eigene Darstellung / olmogo AG.

**1. Loss of Governance:**
Bedingt durch die vollständige Auslagerung des Datenmanagements an den Provider, werden an diesen auch alle Sicherheitsaufgaben übergeben. Dies führt zu einem vollständigen Verlust der Hoheit des Eigentümers über seine gespeicherten Daten.

**2. Malicious Insider:**
Die bewusste Aufgabe dieser Datenhoheit setzt erhebliches Vertrauen in den Serviceprovider voraus. Genau hier liegt das Problem des bösartigen Insiders. Ein Mitarbeiter mit High-Level-




Privilegien missbraucht seine Stellung und verschafft sich unbefugten Zugriff auf Daten.

**3. Isolation Failure:**
Bei diesem Risiko werden durch Fehler in der Infrastruktur Daten des einen Kunden einem anderen zugänglich.

**4. Insecure or incomplete Data Deletion:**
Kundendaten werden z.B. nach Kündigung des Servicevertrags nicht oder unvollständig gelöscht und werden so potenziell Dritten zugänglich.

## Anforderungen an das System der Zukunft

Getreu dem Motto „Sicherheit ist, wenn man nur sich selbst vertrauen muss“ sollte die Lösung der Zukunft den Nutzer unabhängig machen von Vertrauen in Serviceanbieter und IT-Infrastruktur. Die Kontrolle über die eigenen Daten muss immer in den Händen des Inhabers bleiben.

Wie weiter oben im Vergleich mit der analogen Welt gezeigt wurde, ist diese Kontrolle nur möglich, indem der Inhaber der Daten auch selbst diese Kontrolle wahrnimmt; im Beispiel oben also selbst den Schlüssel zu seinem Büro verwaltet.

Diese Aufgabe ist bei herkömmlichen Systemen mit einer erheblichen Einschränkung der Bedienerfreundlichkeit verbunden, die so weit geht, dass eine Nutzung unzumutbar würde.

## Ein patentiertes Verfahren setzt neue Standards

Die Schweizer olmogo AG hat, basierend auf einem patentierten Verfahren, eine Softwarelösung entwickelt, die durch konsequente clientseitige Verschlüsselung aller Nutzerdaten sicherstellt, dass keinerlei lesbare Informationen der Infrastruktur oder dem Provider sichtbar werden können. Das Prinzip, das sich „zero information principle“ nennt, garantiert hundertprozentige Datensicherheit außerhalb des Nutzerendgeräts.

Dabei kümmert sich die Software olmogo um sämtliche Aufgaben der Verschlüsselung, das Verwalten der Schlüssel und der (verschlüsselten) Datenpakete.

## Mühelos für dich, komplexe Technologien im Hintergrund

Basierend auf einem hochskalierbaren Software-Framework, bietet olmogo Lösungen für die folgenden Anwendungsbereiche:

- hochsichere Cloud
- Management von Unternehmensdaten
- Unternehmens-Workspace
- Datenschutz DSGVO
- IoT-Datenmanagement

Nahezu alle Unternehmen haben sensible Daten, die absolut sicher gespeichert und Berechtigten zugänglich gemacht werden sollen. Mit der Software olmogo S3 wurde die Cloud neu gedacht.

> Faktisch sind heutzutage die Datensicherheit und damit die Datenhoheit die zentralen Herausforderungen.

Vollkommen nahtlos integriert sich olmogo S3 in die gewohnte Oberfläche des Betriebssystems und macht hundertprozentig sicheres Speichern und Teilen möglich.

### Auch Nachrichten sind Daten, die geteilt werden sollen

olmogo hat die Sicht auf Daten und deren Management neu definiert. So sind auch Nachrichten (E-Mails oder Chats) Information, die geteilt werden soll. olmogo unterscheidet also konsequenterweise nicht zwischen einem Geschäftsbericht im pdf-Format und einer kurzen Nachricht. Alles sind Daten, mogos genannt, die ein Stück Information von beliebiger Größe, Format und Ursprung enthalten. Sie werden zu null Information verschlüsselt und sind nicht veränderbar. Sie lassen sich beliebig verknüpfen, um Hierarchien und vielteilige Dokumente abzubilden. mogos lassen sich mit ausgewählten Personen oder Einrichtungen teilen. Das System in dem alle mogos leben heißt olmogo.

Gehostet werden kann die Cloud bei olmogo, im eigenen Unternehmen oder einem beliebigen Drittanbieter.

Für Unternehmen, die der Zukunft des Datenmanagements schon einen Schritt näher sein wollen, gibt es den olmogo Workspace. Eine leistungsstarke App, die mit ihrer dynamischen intelligenten Benutzeroberfläche das Speichern und Teilen von Daten und das Schreiben von Nachrichten mühelos und intuitiv erledigt.

### Auch Nachrichten sind Daten, die geteilt werden sollen

Datenschutz im Rahmen der DSGVO und auch das Datenmanagement von IoT-Daten sind komplexe Felder, die kundenspezifische Lösungen benötigen. olmogo M3 ist eine Middleware, die sich in bestehende Unternehmens-IT einfügen lässt. Ausgeklügelte Bibliotheken ermöglichen Programmierschnittstellen zu externen Systemen und erlauben die Integration von olmogo M3 ohne auf eigene Interfaces oder Lösungen verzichten zu müssen.

Da olmogo ein stringentes Konzept von eigentümerbezogener Datenhoheit verfolgt, sind die DSGVO-Anforderungen für Zugriff und Auswertungen implizit erfüllt. Zudem ist olmogo dafür ausgelegt, Massendaten aus dem Internet der Dinge zu verwalten. Eine flexible, zeitbasierte Verschlüsselung dient der Sicherheit, intelligente Agenten überwachen Datenströme und -werte.

### Die Werte der olmogo AG

olmogo hat es sich zur Aufgabe gemacht, den Bedürfnissen nach Sicherheit und Privatsphäre eine neue Plattform zu geben. Der Grundsatz ist: Daten gehören nur dem Eigentümer. Allen anderen – auch olmogo – ist der Zugriff verwehrt. ■

**DR. ALY SABRI,** CEO der olmogo AG in Baar, Schweiz.