E-BOOK

Datenschutz und Datensicherheit

So wird für Sie die Cloud zur sicheren Erfolgsgeschichte

Inhalt

Kapitel 1
Datenschutz und Datensicherheit – Einführung

Kapitel 2
Anwendungsbereiche des Datenschutzrechtes bei Cloud Computing

Kapitel 3
Branchenspezifische Besonderheiten: Buchhaltung

Datenschutz und Datensicherheit – Einführung

Aufgeschreckt durch spektakuläre Datenlecks bei Dropbox, eBay, Sony und sogar Banken sind Unternehmen, Organisationen und Behörden heute deutlich sensibler, wenn es um Datendiebstahl geht. Wesentlich mehr Privatpersonen wollen wissen, was mit ihren Daten passiert. Am Anfang der Digitalisierung hieß Datenschutz: Eine Excel-Tabelle mit einem Passwort zu versehen. Unter Datensicherheit verstand man, bei Feierabend die Tür zum Serverraum abzuschließen.

Das ist Datenschutz

Laut der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) garantiert Datenschutz „jedem Bürger Schutz vor missbräuchlicher Datenverarbeitung, das Recht auf informationelle Selbstbestimmung und den Schutz der Privatsphäre." Datenschutz ist demnach ein Recht jeder Bürgerin und jedes Bürgers, bei dessen Missachtung gleichzeitig die Persönlichkeitsrechte und Grundrechte von Menschen verletzt werden. Es ist also keinesfalls trivial, fahrlässig mit personenbezogenen Daten umzugehen.

Das ist Datensicherheit

Die Datensicherheit betrifft alle Daten, unabhängig davon, ob diese personenbezogen sind oder nicht. Daher fallen nicht nur personenbezogene Daten darunter, sondern zum Beispiel auch Finanz- und Warenwirtschaftsdaten, interne Statistiken und Strategiepapiere, Konstruktionspläne und Rezepturen. Datensicherheit hat das Ziel, Daten jeder Art durch technische und organisatorische Maßnahmen gegen Verlust, Manipulation, unberechtigte Kenntnisnahme durch Dritte oder andere Bedrohungen zu sichern.

Ein altes Thema

Datenschutz ist durch die Digitalisierung, Big Data und Cloud Computing stärker in den Fokus geraten. Datensicherheit hingegen ist in dieser Breite ein vergleichsweise junges Thema, das vom operativen Management wegen seiner Abstraktheit lange stiefmütterlich behandelt wurde. Die Digitalisierung machte große Datenmengen leicht und unmerklich kopierbar; das Internet schuf neue Angriffsflächen. Es wäre aber falsch anzunehmen, dass Datenschutz ein rechtliches und Datensicherheit ein technisches Problem wäre. Beide Themen sind eng miteinander verknüpft und spielen technisch und juristisch eine große Rolle – vom Business-Design bis zum Tagesgeschäft des Angestellten.

Anwendungsbereiche des Datenschutzrechtes bei Cloud Computing

Dem vergleichsweise laxen Datenschutz in den USA steht der strenge europäische Datenschutz gegenüber. Vieles, was Produkte von US-Anbietern dem Anwender ermöglichen, ist in der EU und mit den Daten von EU-Bürgern schlicht verboten. Und die EU zieht die Schrauben weiter an: Mit der General Data Protection Regulation (GDPR), auf Deutsch Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 in Kraft ist, wurde die Datenschutz-Richtlinie aus den 1990er Jahren abgelöst. Die DSGVO ist umfassender, genauer und restriktiver. Und sie ist kein Papiertiger: Verstöße werden geahndet mit bis zu 20 Millionen Euro oder bis zu 4 Prozent des Jahresumsatzes – je nachdem, welcher Wert höher ist. Die Bußgeldregelung zeigt allen Unternehmen am Markt unmissverständlich, dass es der Regierung mit dem Datenschutz ernst ist.

Datenschutz und -sicherheit sollten heute von Anfang an berücksichtigt werden, wenn man Geschäftsprozesse, Software und IT-Infrastrukturen entwickelt. Dabei sind die Anforderungen hoch – zu hoch für viele kleine und mittelgroße Unternehmen, als dass sie diese in Eigenregie verwirklichen und dabei ruhig schlafen könnten. Meist hat sich in einem Unternehmen im Laufe der Jahre auch ein schierer Zoo von Geschäftsanwendungen angesammelt – eine weitere große Hürde bei der Umsetzung der DSGVO. Die Regulierung fordert, dass ein Unternehmen genau sagen kann, welche personenbezogenen Daten bei ihm gespeichert sind, wie sie eingesetzt werden, ob Einverständnisse vorliegen und jeder einzelne Datensatz auf Wunsch des Dateneigentümers unternehmensweit gelöscht werden kann. In den vergangenen Jahren hatten Unternehmen die IT-Struktur nicht mehr ganz im Haus, sondern sie nutzen heute vermehrt Cloud-Dienste und Virtualisierung. Die IT-Anbieter mussten ihre Produkte in puncto Datenschutz und Datensicherheit auf die Höhe der Zeit bringen und das taten sie – als Cloud-Anbieter für alle Kunden. Entsprechend groß ist hier die Sorgfalt.

Für viele Firmen jeder Größe ist es damit noch interessanter, große Teile ihrer IT in die Cloud zu verlegen. Sie delegieren damit Datenschutz und -sicherheit größtenteils und machen sie kalkulierbarer. Wer den richtigen Anbieter wählt, kombiniert so die große Flexibilität der Cloud mit Datenschutz und -sicherheit in den Händen von Profis.

Cloud-Services – kleiner Auszug der Möglichkeiten

„Software as a Service" (SaaS): Beim Klassiker des Cloud-Geschäfts liegt die Software praktisch komplett auf den Servern des Cloud-Anbieters. Auf dem Arbeitsplatzrechner des Anwenders dient meist nur der Webbrowser als Benutzeroberfläche für die Anwendungen, so dass man überall dort arbeiten kann, wo eine Verbindung zum Internet besteht.

„Infrastructure as a Service" (IaaS): Wer auch seine sonstigen Server auslagern möchte, kann per IaaS Server anmieten.

„Platform as a Service" (PaaS): Ihr Unternehmen erhält eine ganze **Plattform**, auf der man eigene Webanwendungen entwickeln und betreiben kann. Darüber hinaus gibt es **CaaS** für die Telekommunikation, **HuaaS** für Dienstleistungen, die nach wie vor Humanressourcen benötigen, sowie **HPCaaS** und **DICaaS** für „high performance" und „data intensive computing".

Kernpunkte zur Auswahl eines Cloud-Anbieters

Gleich vorneweg: Abzuraten ist von einem Ad-hoc-Umstieg auf einen Cloud-Dienst. Selbst für kleinere Projekte ist dies nicht ratsam, da sie die Zahl der verwendeten Systeme eher vergrößert und damit die nötige Datenübersicht verringert, statt zu erhöhen.

Eine Publikation des Bundesamts für Sicherheit in der Informationstechnik (BSI) gibt einen Leitfaden an die Hand, wie Unternehmen, Organisationen und Behörden die Nutzung von Cloud Computing am besten planen, umsetzen und langfristig entwickeln.

Die Cloud-Strategie entwerfen

Erst einmal sollten Sie die Anforderungen und Rahmenbedingungen des betroffenen Geschäftsfeldes definieren.

Gründen Sie ein Projektteam mit Entscheidern aus den betroffenen Unternehmensbereichen. Skizzieren Sie in diesem Gremium die Ausgangslage im Unternehmen und den gewünschten Nutzen, den das Cloud-Projekt bringen soll. Legen Sie außerdem fest, welcher Dienst, welches Service-Modell und welches Bereitstellungsmodell untersucht werden soll. Auch falls unter den Beteiligten des Projekts schon Vorlieben bestehen: Vermeiden Sie, sich hier schon festzulegen, denn die Wahl des passenden Anbieters soll das Ziel und nicht die Anfangsbedingung sein.

Das Projektteam erstellt eine **Machbarkeitsstudie**, die mehrere Punkte beleuchtet:

- Welche Art von Daten sollen in der Cloud verarbeitet werden und dürfen diese überhaupt in eine Cloud? So dürfen beispielsweise steuerlich relevante Daten nur nach Genehmigung durch das Finanzamt im Ausland gespeichert werden und dann auch nur innerhalb des EU- oder EWR-Raums.
- Ist Ihre IT in der Lage, Cloud-Dienste einzuführen und zu nutzen? Oder welche Dienste kann sie nutzen?
- Ist die Infrastruktur inner- und außerhalb des Unternehmens für die angestrebte Cloud-Nutzung ausgelegt? Hier sind besonders Bandbreite und Zuverlässigkeit der Internetanbindung wichtig.
- Achten Sie auf Sicherheitszertifikate des Rechenzentrum-Anbieters, damit die sensiblen Informationen über einen sicheren Cloud-Zugang abgesichert sind.
- Überprüfung der Rechte und Verschlüsselung, beispielsweise durch die Umleitung von SMS als Authentifizierungsfaktor, damit Sie vor unberechtigten Angriffen geschützt sind.

Die Ergebnisse der Machbarkeitsstudie stecken das Feld der in Frage kommenden Service- und Bereitstellungsmodelle ab.

Kleine Cloud-Kunde

Public Cloud
Das Angebot richtet sich an die Allgemeinheit oder eine große Zielgruppe, zum Beispiel eine ganze Branche. Die Infrastruktur ist im Besitz des Anbieters, nicht des Kunden.

Private Cloud
Die Infrastruktur und der Betrieb liegt beim Nutzer. Meist greift man dabei auf die Software und das Know-how eines Dienstleisters zurück. Diese Form erreicht in aller Regel nicht das gute Flexibilitäts-Kosten-Verhältnis wie eine Public Cloud, kann aber aus Gründen des Datenschutzes und der Datensicherheit erforderlich sein.

Hybrid Cloud
Bei dieser Mischform laufen bestimmte Services bei externen Anbietern über das Internet, während besonders kritische Daten im Unternehmen gespeichert und verarbeitet werden.

Community Cloud
Diese Form liegt vor, wenn mehrere Unternehmen oder Organisationen gemeinsam einen Cloud-Dienst einrichten und exklusiv nutzen.

Es folgt eine Risiko-Analyse, in der alle Datenarten hinsichtlich deren Schutzbedarfs klassifiziert werden. Für die Einstufung entscheidend sind dabei drei getrennt zu bewertende Kriterien:

- Vertraulichkeit: Schaden bei Verlust der Daten
- Integrität: Schaden bei Veränderung der Daten
- Verfügbarkeit: Schaden bei Nicht-Verfügbarkeit der Daten

Dabei sind folgende Gefährdungen besonders relevant:

- Zugriff auf die Daten durch den Cloud-Anbieter selbst
- Behördlicher Zugriff durch juristische Verfügung im Rechtsraum, dem der Cloud-Anbieter unterliegt
- Kompromittierung der Authentifizierung (Passwort-Diebstahl, Computer-Einbruch, ...)
- Datenverlust
- Datenmanipulation

Die Risiko-Analyse zeigt, wo besondere Sicherheitsmaßnahmen notwendig werden und welche neuen Risiken entstehen, die nicht behandelt werden können. Absolute Sicherheit gibt es auch bei Cloud-Anbietern nicht, aber eine sehr hohe Sicherheit. Die Risiko-Lage ist mit der folgenden Kosten-Nutzen-Analyse zu bewerten.

Als Drittes erstellt das Team eine grobe **Kosten-Nutzen-Abschätzung**. Sie sollte gut und realistisch, aber zu diesem Zeitpunkt noch nicht zu detailliert sein. Sie soll einen ersten Eindruck davon vermitteln, ob sich ein Wechsel in die Cloud lohnen könnte. Berücksichtigen sollte sie zumindest die Kosten des Diensts, den internen Administrationsaufwand, die Schulung von Mitarbeitern und Administratoren, die Kosten für neue IT-Infrastruktur und größere Bandbreiten, die Kosten von Prozessanpassungen und die Migration sowie zu erwartende interne Einsparungen.

Sicherheitsanforderungen identifizieren

Entscheidet man sich auf der Basis der gemachten Untersuchungen dazu, das Projekt weiterzuverfolgen, werden die Schritte konkreter.

Nun ist der Zeitpunkt gekommen, die **funktionalen Anforderungen** festzustellen. Dieser, in der Regel eher umfangreichere Teil, sollte auch dazu genutzt werden, die Geschäftsprozesse auf DSGVO-Konformität zu überprüfen.

Die schon erstellte grobe **Risikoanalyse** muss jetzt verfeinert werden. Wenn schon eine Risiko- und Sicherheitsanalyse im Haus vorliegt – was so sein sollte – ziehen Sie diese dafür hinzu. Ebenfalls relevant sind rechtliche Vorgaben. Greifen Sie dabei auf die oben erwähnte Klassifikation der Informationen zurück. Aus dem Ergebnis dieser Analyse werden Sie die Anforderungen ableiten, die Sie an den Cloud-Anbieter hinsichtlich Sicherheit und Verfügbarkeit stellen müssen.

Erstellen Sie einen vereinfachten Plan, der Auskunft über die beteiligten Personengruppen, die Kommunikationsverbindungen sowie die IT-Systeme gibt und zwar sowohl auf Seiten Ihres Unternehmens als auch auf Seiten des Cloud-Anbieters.

Ermitteln Sie die **Angriffsvektoren**, also die möglichen Wege, wie Unberechtigte auf die Daten zugreifen könnten oder wie Sie als Unternehmen daran gehindert werden könnten, auf den Dienst und Ihre Daten zuzugreifen. Eine wichtige Rolle spielen hier zum Beispiel, wie sicher die Arbeitsplatzrechner gegen Passwort-Diebstahl sind, die Passwort-Richtlinie des Unternehmens, ob das Verbindungsprotokoll nach aktuellem Stand sicher ist, ob interne Hard- und Software-Infrastruktur regelmäßig Sicherheits-Patches bekommen.

Filtern Sie aus diesen Erkenntnissen die wichtigsten Angriffsvektoren zu einer Sicherheitsrichtlinie, die Anforderungen formuliert. So lange nicht zwingende Gründe vorliegen, sollten die konkreten Maßnahmen jedoch noch offen bleiben.

Jetzt ist die Zeit für eine Zwischenbilanz. Public Cloud ermöglicht Ihnen die benötigte Infrastruktur und schnelle Implementierung der Services im Unternehmen, unter Einhaltung der hohen Sicherheitsansprüche vom Rechenzentrum. So muss sich das IT-Team nicht mehr mit Hardware und Bandbreitenfragen auseinandersetzen und kann sicher sein, dass die sensiblen Daten geschützt werden.

Services, Schnittstellen und Verantwortungsbereiche definieren

Unter den Mitarbeitern von Unternehmen, Organisationen und Behörden zählt die Dokumentation der Prozesse zu den weniger beliebten Aufgaben. Dennoch sind solche Dokumente hilfreich, wenn es darum geht darzustellen, was für Services die Cloud bieten muss. Ohne einen konkreten Katalog funktionaler Merkmale ist keine Anbieter-Auswahl möglich. Zusammen mit den Sicherheitsanforderungen ergibt sich erst das Bild eines geeigneten Dienstes.

Cloud-Dienste werden über Schnittstellen genutzt, beginnend beim Web-Browser des Mitarbeiters Ihres Unternehmens bis zu Anbindungen an bestehende Systeme wie Warenwirtschaft und andere Cloud-Dienste. Ermitteln Sie, welche Anforderungen hier bestehen (zum Beispiel gibt es auf Linux-Rechnern keinen Microsoft Internet Explorer) beziehungsweise welcher Spielraum auf Ihrer Seite besteht (Standard-Schnittstellen und -Protokolle).

Klären Sie, wo genau die Linie zwischen Cloud-Dienst und Cloud-Nutzer, also Ihrem Unternehmen, liegt. Spätestens wenn bei der Migration oder im Betrieb Probleme auftreten, muss klar sein, in wessen Spielfeld der Ball liegt.

Bei allen Anforderungen sollten Sie unterscheiden zwischen „must have“ und „nice to have“. Andernfalls werden Kompromisse bei der Anbieterauswahl praktisch unmöglich.

Wichtig: Verlassen Sie sich nicht auf unverbindliche Zusagen bei Features und Schnittstellen. Ob „Beta-Stadium“ oder „in Planung“ – nur schriftlich belegte, vollumfängliche Eigenschaften mit langfristiger Unterstützung zählen.

Migration und IT-Infrastruktur planen

Es mag zu früh erscheinen, noch vor der Entscheidung für einen Anbieter einen **Migrationsplan** zu erstellen. Aber es hat sich gezeigt, dass auf dem praktischen Weg in die Cloud beträchtliche und sogar unüberwindliche Hürden liegen können.

Sofern es ein Vorgänger-System gibt, ist der wichtigste Punkt die Migration der Daten. Klären Sie, über welche Schnittstelle (meist XML- und CSV-Formate) die Daten aus bestehenden Systemen abgezogen werden können und welche Berechtigungen dafür nötig sind. Legen Sie fest, wie der Erfolg der Migration geprüft werden kann.

Schätzen Sie ab, wie umfangreich die Änderungen an den Geschäftsprozessen sein werden und wie die Mitarbeiter darauf vorbereitet werden können (Schulungsplan).

Bei jedem dieser Punkte kann es sinnvoll sein, für die Umsetzung einen externen Dienstleister hinzuzuziehen, damit das System zügig eingeführt werden kann.

Eine schnelle Umstellung auf den Cloud-Dienst wird auch dadurch unterstützt, dass Sie frühzeitig planen, was an der **IT-Infrastruktur** durch die Cloud-Nutzung geändert werden muss. Welche Hardware muss ausgetauscht werden (Proxys, Router, Load Balancer, etc.)? Müssen eventuell Betriebsschnittstellen und Versorgungsskripte entwickelt werden? Brauchen Sie für eine größere Bandbreite beim Internet-Versorger einen anderen Vertrag oder müssen Sie den Versorger sogar wechseln?

All diese Komponenten werden in der Regel nicht über Nacht geliefert, programmiert beziehungsweise umgestellt. Planen Sie dafür ausreichend Zeit ein.

Sicherheitskonzept aktualisieren

Im IT-Sicherheitskonzept eines Unternehmens sollten alle sicherheitsrelevanten Punkte festgehalten sein. Der Einsatz von Cloud-Technologien macht deutliche Änderungen am Konzept nötig. Insbesondere werden die Sicherheitskonzepte des Cloud-Anbieters und auch des Netzanbieters Teil des Konzepts, stellen doch beide Anbieter dann einen virtuellen Teil des Unternehmens dar. Die zuvor erstellte Risiko-Analyse und die identifizierten Angriffsvektoren können als Grundlage dienen.

Im Konzept werden auch Sicherheits-Maßnahmen beschrieben wie beispielsweise mit sicherheitsrelevanten Vorfällen umzugehen ist, welche Administrationsfälle ein Vier-Augen-Prinzip erfordern, welche Monitorings zu etablieren sind, kryptografische Mindeststandards, Backup-Regelungen beim Cloud-Anbieter und -Nutzer. Audits sind hier das bewährte Mittel, um zu überprüfen, ob alle beteiligten Seiten das Konzept einhalten.

Bei der Cloud-Nutzung ist es eher der Normalfall, dass auch personenbezogene Daten verarbeitet werden. Auch wenn Sie Ihre Daten zum Cloud-Anbieter auslagern, bleibt – laut Gesetz – die Verantwortlichkeit für den Schutz personenbezogener Daten gegenüber dem Inhaber bei Ihnen und geht nicht auf den Cloud-Anbieter über. Sie sind verpflichtet, den Anbieter sorgfältig auszuwählen und auch während der Nutzung für die Einhaltung der Vereinbarungen zu sorgen. Insbesondere Behörden unterliegen hier strengen und abgestuften Regeln. Grundsätzlich gilt: je sensibler die Daten, desto restriktiver sind die Regelungen. Das BSI hält rund um das Thema IT-Grundschutz eine Reihe von Publikationen bereit[1].

[1] Alle Dokumente zum IT-Grundschutz des BSI, www.bsi.bund.de/grundschutz

Cloud-Anbieter auswählen

Die bis hierhin geleistete Vorarbeit zahlt sich nun aus. Die Beschreibung des gewünschten Cloud-Dienstes und das Sicherheitskonzept können nun in ein Lastenheft beziehungsweise eine Leistungsbeschreibung einfließen.

In der Praxis werden insbesondere Zertifikate und Testate, die der Cloud-Anbieter vorweisen kann, darüber entscheiden, ob er die Sicherheitsanforderungen erfüllt. Hierbei ist es allerdings wichtig zu prüfen:

- Bezieht sich das Zertifikat/Testat auf relevante Services?
- Was ist genau der Gegenstand des Zertifikats/Testats und was ist seine letztliche Aussage?

Ob sich ein Anbieter eignet, sollte insbesondere an folgenden Kriterien festgemacht werden:

- Reputation und überprüfbare Referenzen
- Bewertungen von (möglichst unabhängigen) Organisationen
- Ist Cloud Computing ein langfristiges Geschäftsfeld oder gar das Kerngeschäft?
- An welchen Standorten findet die Datenspeicherung und -verarbeitung statt?
- Welchem Recht unterliegt der Anbieter und welches Recht liegt einem Vertrag mit ihm zugrunde?
- Inwieweit können und dürfen der Dienstanbieter oder Dritte (zum Beispiel staatliche Behörden) auf die Daten zugreifen?
- Welche Subunternehmer sind an der Leistungserbringung beteiligt beziehungsweise in welchen Abhängigkeiten steht der Dienstanbieter?
- Welche Möglichkeiten gibt es, die Angaben des Anbieters zu verifizieren?

Gerade bei der Frage, wo die Daten lagern und inwieweit Behörden darauf zugreifen können, sind durch die europäische DSGVO keine Kompromisse möglich.

Hat ein Cloud-Anbieter die Hürden der funktionalen und sicherheitstechnischen Anforderungen genommen, erstellen Sie für dessen Angebot eine detaillierte Kosten-Nutzen-Analyse, in die auch die Schulungen eingehen. Auch Kosten für die spätere Migration zu einem anderen Anbieter oder zurück ins Haus sollten beziffert werden.

Nun kann entschieden werden, welcher Anbieter zum Zug kommt oder ob das Projekt mangels passender Angebote abgebrochen werden muss.

Der Vertrag mit dem Cloud-Anbieter

Bevor der Weg in die Cloud durch eine Beauftragung tatsächlich starten kann, sind der vom Anbieter vorgelegte Vertrag und dessen AGB zu prüfen.

Da es sich um eine strategische und hoffentlich längerfristige Bindung handelt, versteht sich eine eingehende Prüfung von selbst. Achten Sie insbesondere auf Folgendes:

- Ort der Leistungserbringung
- Beteiligte Subunternehmer
- Einhaltung von Sicherheitsanforderungen (der BSI Anforderungskatalog „Cloud Computing C5" sollte das Minimum darstellen[2])
- Infrastruktur des Cloud-Anbieters
- Personal (Sicherheitseinstufung, Verpflichtung auf das Datengeheimnis)
- Eindeutige Kommunikationswege und Ansprechpartner
- Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten
- Ggf. besondere Regelung bei Sicherheitsvorfällen oder Betriebsunterbrechungen beim Cloud-Anbieter (zum Beispiel Zugriff auf Log-Dateien)
- Notfallvorsorge
- Änderungsmanagement
- Kontrollen (regelmäßige Prüfungen und Berichte)
- Regelungen zu rechtlichen Rahmenbedingungen
- Vertragsstrafen bei Nichterfüllung
- Haftungsfragen
- Beendigung und Datenlöschung

[2] Anforderungskatalog Cloud Computing (C5) des BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.html

Mit dem Cloud Computing profitieren nicht zuletzt Sie als Kunde vom Kostenvorteil durch Standardisierung. Dies bringt allerdings mit sich, dass auch die Service Level Agreements (SLA) und Operational Level Agreements (OLA) meist fix sind. Im Gegensatz zu Privatkunden können Geschäftskunden eher verhandeln und beim Thema Datensicherheit müssen sie auch oft auf ihren Sicherheitsvorgaben bestehen. Die Anbieter wissen auch, dass die Kunden hier immer sensibler werden und werben oft mit besonders hohen Standards – diese müssen sich allerdings belegen lassen.

Wenn personenbezogene Daten in die Cloud wandern sollen, müssen Sie mit dem Anbieter einen Vertrag zur Auftragsdatenverarbeitung (ADV) nach § 11 BDSG abschließen. Wie bereits erwähnt, verbleibt aber die Verantwortung für den Datenschutz bei Ihnen. Die Sicherheitsrichtlinien Ihres Unternehmens und die Vereinbarungen mit dem Cloud-Anbieter müssen sicherstellen, dass den Daten der adäquate Schutz durchgehend zukommt – von der Migration in die Cloud bis zum Ende des Dienstleistungsverhältnisses.

Migration und Betrieb

Die Migration auf den Cloud-Dienst verläuft ähnlich wie jeder Wechsel auf eine neue zentrale Software: In einem mehrstufigen Test- und Pilotbetrieb, in dem ausgewählte Mitarbeiter mit dem neuen System arbeiten, wird festgestellt, ob die migrierten Daten korrekt sind, die Funktionalität und die Leistungsfähigkeit stimmen und welche Prozessbeschreibungen und Richtlinien angepasst werden müssen. Mit Protokollen, Reportings und Reviews stellen Sie fest, wie fit Ihre Mitarbeiter sind und ob der Dienstleister sein versprochenes Service-Level erreicht. Sammeln Sie die auflaufenden Schwierigkeiten und Kritikpunkte und bringen Sie sie in regelmäßigen Abstimmungsrunden mit dem Dienstleister auf den Tisch. Auch nachdem Sie erfolgreich produktiv gegangen sind, sollten Sie einen engen und regelmäßigen Kontakt zum Dienstleister pflegen.

Branchenspezifische Besonderheiten: Buchhaltung

Die Buchhaltung ist aufgrund des rechtlichen und regulatorischen Rahmens stark standardisiert und damit besonders gut für die Cloud geeignet. Der Nutzer profitiert davon durch niedrige Kosten und durch stark optimierte Prozesse, die das Rechnungswesen insbesondere für Unternehmer ohne Vollzeitbuchhalter erleichtern.

Bei der Auswahl eines „Cloud Accounting"-Angebots sollte man einen Blick über den Zaun und in die Zukunft werfen. Es kann sinnvoll sein, auf Schnittstellen zu anderen Bereichen wie Lohn- und Gehaltsabrechnungen zu achten, um einer weiteren Integration keine Steine in den Weg zu legen. Oft kann der Anbieter auch in den anderen Bereichen mit Produkten aufwarten, die sich nahtlos zusammenfügen lassen.

Zu den Anforderungen an Datensicherheit und Datenschutz gemäß der DSGVO kommt noch die Anforderung des deutschen Fiskus: Steuerlich relevante Daten dürfen wie bereits gesagt nur nach Genehmigung durch das Finanzamt im Ausland gespeichert werden und dann auch nur innerhalb des EU- oder EWR-Raums.

Aus diesem Grund scheiden viele Anbieter aus Übersee aus, denn diese machen sich bislang kaum die Mühe, eigene Rechenzentren in Europa aufzubauen und dann ihre Software auch noch auf die Gesetzgebung im jeweiligen Land anzupassen. Letzteres ist nötig, wenn der Dienst vorschriftsmäßige Rechnungen stellen, mit verschiedenen Mehrwertsteuersätzen umgehen und rechtskonforme Bilanzen oder Gewinn-und-Verlust-Rechnungen ausgeben soll. Selbst wenn die Benutzeroberflächen durchgehend sprachlich übersetzt sind, haben viele Angebote aus Übersee hier Mängel. Daher sollten Sie nur Angebote von Anbietern nutzen, die belegen können, dass sie ihren Dienst auf deutsche Gegebenheiten zugeschnitten haben.

Auch bei der Sicherheit Ihrer Finanzbuchhaltungsdaten gilt, was für den Schutz personenbezogener Daten gilt: Auch mit einem Cloud-Dienst sind Sie – nicht Ihr Dienstleister – für die Sicherheit und den Schutz verantwortlich. Die Datensicherheit gilt als Teil der ordnungsgemäßen Buchführung. Gehen Daten unwiederbringlich verloren, kann eine Steuerprüfung die Buchführung im Zweifelsfall verwerfen und die Besteuerungsgrundlagen schätzen.

Gute Cloud-Anbieter unternehmen sehr viel für Datensicherheit und Datenschutz und liegen in der praktischen Sicherheit oft höher als Unternehmen mit eigener IT und abgehefteter Sicherheitsrichtlinie. Da Unternehmen auch bei klassischer Buchhaltungssoftware in aller Regel auf Standardprodukte setzen, ist ein Wechsel in die Cloud für die Buchhaltung meist um ein Vielfaches leichter als bei den Prozessen des Kerngeschäfts.

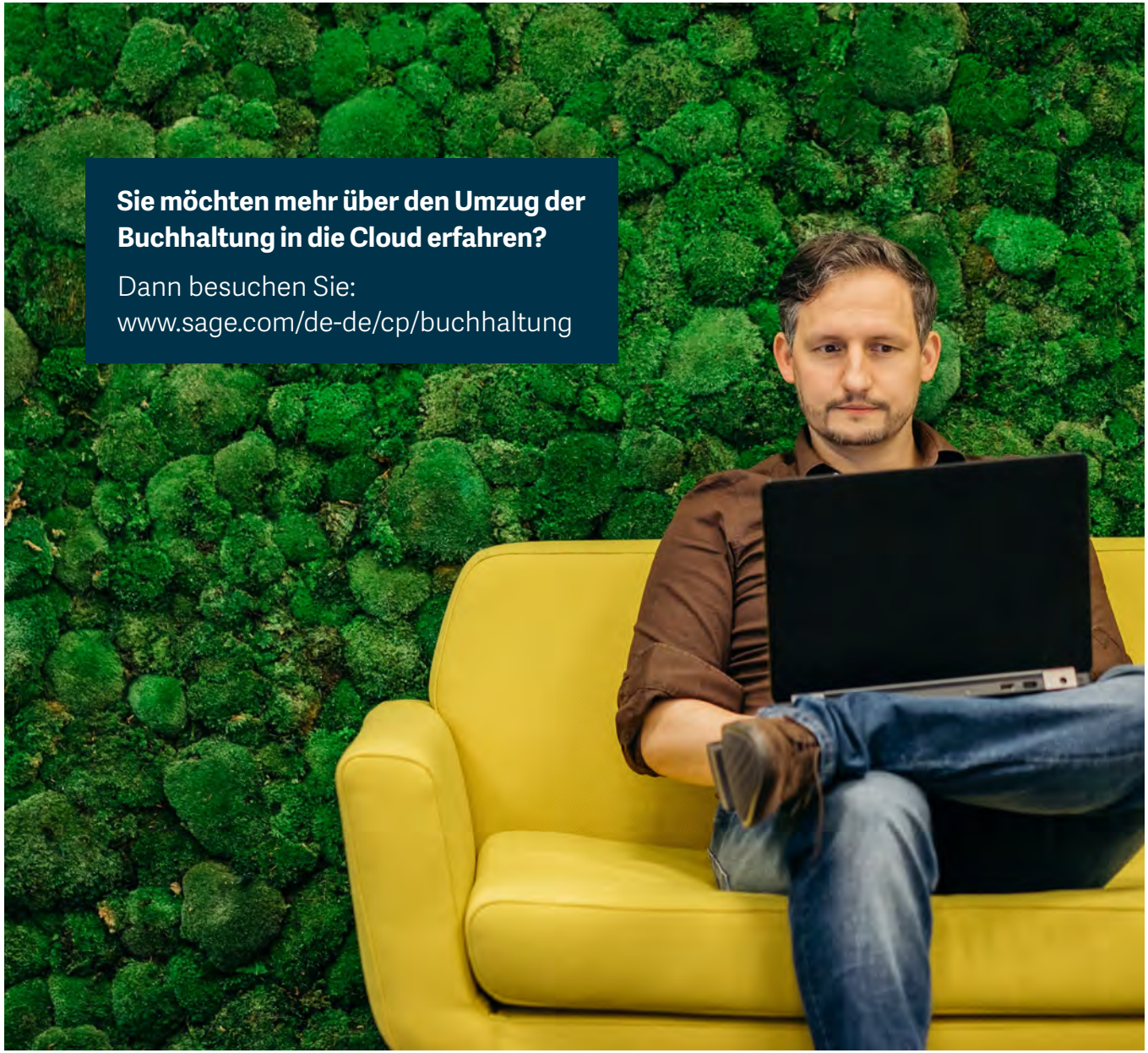
Cyber-Security bei Cloud-Diensten

Die klassischen Gefahren für Ihre Daten sind Verlust, Manipulation und Diebstahl. Cloud-Dienste sind dabei besonders im Visier von Kriminellen und Spionage. Aber gerade deshalb unternehmen Cloud-Dienste enorme Anstrengungen, um für diese Gefahren gewappnet zu sein, angefangen von mehrfach redundanter, räumlich verteilter Speicherung über strenge und regelmäßige Audits bis hin zu Angriffsabwehrabteilungen, die bei Cyber-Security auf dem neuesten Stand sind.

Bei der Cloud-Nutzung kommt die Gefahr hinzu, dass Sie auf Ihre Daten nicht zugreifen können:

- Ausfall der Internetanbindung Ihres Unternehmens beziehungsweise Ihrer Organisation oder Behörde. Hier ist der Internet-Provider in der Pflicht.
- Daten können auf dem Weg durch das Netz abgefangen und ausgespäht werden. Daher muss auf der gesamten Strecke zwischen Unternehmen und Cloud-Anbieter Authentifizierungs- und Verschlüsselungstechnik zum Einsatz kommen, die nach aktuellem Stand als ausreichend sicher gilt.
- Kriminell motiviertes massives Anfrage-Bombardement durch fremde Rechner können die Cloud-Server so auslasten, dass sie für die eigentlichen Nutzer nicht mehr erreichbar sind (Distributed Denial of Service Attack, DDoS).

Letztere nehmen seit Jahren stetig und deutlich zu. Die Anbieter von Cloud-Services und die Betreiber großer Webseiten arbeiten eng mit den Internet-Providern zusammen, die den Datenverkehr bei erkannter DDoS-Attacke durch spezielle Technik filtern können und damit den Schaden so klein wie möglich halten.



Sage GmbH
Franklinstraße 61-63
D-60486 Frankfurt am Main

T: +49 69 50007-6300
E-Mail: info@sage.de

www.sage.com

©2021 Sage GmbH. Alle Rechte vorbehalten. Sage, das Sage Logo sowie die hier genannten Sage Produktnamen sind eingetragene Markennamen der sage Group plc bzw. ihrer Lizenzgeber. Alle anderen Markennamen sind Eigentum der jeweiligen Rechteinhaber. Technische, formale und druckgrafische Änderungen vorbehalten. Stand: März 2021