



Digitalisierung und Datenschutz: So gelingt die **Cloud-Migration**

Wie Sie mit Microsoft 365 und anderen Online-Lösungen datenschutzkonform die Zukunft gestalten

von Matthias Niedung und Thomas Althammer

Digitalisierung hat mit dem Ausbruch des Covid-19 Virus einen Schub unerwarteten Ausmaßes erfahren. Zahlreiche Unternehmen haben den Weg in die Cloud vollzogen oder planen diesen. Damit Sie auch rechtssicher den Weg in die Zukunft gestalten können, haben wir zahlreiche Fakten gesammelt und zeigen auf, wie die Cloud auch Ihren Unternehmenserfolg sichern kann.

Alles Cloud? Cloud verstehen, Risiken erkennen!

Cloud-Angebote gibt es unzählige und vor allem die Anbieter aus Übersee überzeugen mit professionellen Dienstleistungen. Dabei unterscheiden die Anbieter drei wesentliche Bereiche:



Matthias Niedung, Berater für Informationssicherheit und Datenschutz



Thomas Althammer, Geschäftsführer der Althammer & Kill GmbH & Co. KG

Infrastructure as a Service (IaaS) ermöglicht es Ihnen, Ihr komplettes Rechenzentrum vollends virtuell abzubilden und in die Cloud zu verlagern.

Wer nur bestimmte Bereiche virtuell abbilden möchte, kann auf die Angebote des **Plattform as a Service (PaaS)** setzen. Hier werden Ihnen vollständige Betriebssysteme und virtuelle Server zur Verfügung gestellt und diese gewartet.

Die bekanntesten Produkte im Cloud-Umfeld hingegen sind die Produkte aus dem Bereich **Software as a Service**. Microsoft 365 stellt dabei einen der wohl bekanntesten Services dar. Aber auch Projekttools, wie Atlassian Jira, ganze ERP-Lösungen und weitere unternehmensunterstützende Software lässt sich aus der Wolke beziehen. Hier genießen Sie als

Fotos: oben: Bongkarn Thanayakij; Autorenfotos: Christian Wyrwa/Wyrwa Fotografie

Unternehmen den Vorteil, dass Sie sich um Ressourcen nicht kümmern müssen und stets die aktuelle Version der Software zur Verfügung haben.

Doch die permanente Erreichbarkeit der Services birgt ebenfalls Risiken, welchen Sie sich als Unternehmer bewusst sein müssen. Die Schutzziele, Vertrauenswürdigkeit, Verfügbarkeit und Integrität Ihrer Informationen und personenbezogenen Daten, benötigen einen bewussten Blick auf die Risiken, um diese zielgerichtet reduzieren zu können.

Verfügbarkeit

Allem voran steht im Ernstfall die Verfügbarkeit Ihrer Informationen im Fokus. Gerade in Krisenzeiten offenbart sich, wie notwendig die Aufrechterhaltung der Verfügbarkeit für das Überleben des Unternehmens sein kann. Während die Cloud-Struktur die Daten zwar überall prinzipiell verfügbar macht, sind die Voraussetzungen von Unternehmen zu Unternehmen unterschiedlich. Sind Sie beispielsweise in der Lage, eine enorme Datenlast durch den Flaschenhals Internetzugang bereitstellen zu können? Besitzen Ihre Mitarbeiter in den heimischen Gefilden auch tatsächlich die Voraussetzungen, um über das Internet die Informationen auch

verarbeiten zu können? Oder was passiert, wenn auf einer Baustelle vor Ihrer Geschäftsstelle das Glasfaser-Kabel zertrennt wird?

Vertraulichkeit

Besonderes Augenmerk bedarf das Schutzziel der Vertraulichkeit. Während die Verfügbarkeit auch für einen gewissen Zeitraum meistens für Unternehmen als handhabbares Risiko behandelt werden kann, sieht es beim Schutzziel der Vertraulichkeit schon bedeutend gravierender aus. Ein einmaliger Verlust der Vertraulichkeit lässt sich nicht wieder umkehren. Sind Daten also von unberechtigten Personen entdeckt worden, ist das Schutzziel nicht mehr gewährleistet. Gerade im Hinblick auf den Datenschutz hat dies weitreichende Folgen.

Neben dem allgemeinen Zugriff auf Daten durch Außenstehende, sollten Sie demnach ebenfalls ein Rollen- und Berechtigungskonzept entwickeln, was restriktiv regelt, wer, wann und unter welchen Voraussetzungen auf Ihre Informationen zugreifen darf. Zudem sollten Sie alle Risiken betrachten, welche das Schutzziel gefährden. Hierbei sollten auch Fragestellungen berücksichtigt werden, welche den Zugriff auf privaten oder nicht im Unternehmenskontext

Wir stehen für
bedürfnis-
gerechtes
Bodendesign

Im Alter ändern sich die Bedürfnisse – auch an das Wohn-design. Lesen Sie mehr dazu in unserer Studie und laden Sie das kostenlose Whitepaper herunter über den QR-Code oder per E-Mail an info.de@tarkett.com



Eingeschränkte Sicht mit Demenz

 **Tarkett**

Besuchen Sie uns unter www.tarkett.de

So gelingt die Cloud-Migration

bereitgestellten Geräten thematisieren. Übrigens: auch öffentlich verfügbare Backups sind eine Gefahrenquelle für die Vertraulichkeit Ihrer Informationen.

Integrität

Ein weiteres, wesentliches Schutzziel im Datenschutz ist die Integrität von Informationen. Ein nicht unerheblicher Schaden kann auftreten, wenn die Informationen des Unternehmens manipuliert oder verändert werden. Die Auswirkungen sind mitunter gravierend. Nicht integrierte Informationen beherbergen massive Gefahren für den Unternehmenserfolg bis hin zu lebensbedrohlichen Szenarien. Ob Widerspruchsfristen, Skonto-Termine oder eine veränderte Patientenakte, wer die Risiken auf die Integrität der Informationen betrachtet, bewahrt sich vor weitreichenden Folgen.

Zielführend ist es demnach, technische und organisatorische Maßnahmen zu treffen, die eine Veränderung Ihrer Informationen protokollieren, nachvollziehbar machen und böswillige Veränderungen verhindern. Besonderes Augenmerk gilt dann, wenn es um personenbezogene Daten geht, welche Sie in der Cloud verarbeiten wollen.

Datenschutz-Folgenabschätzung erforderlich?

Für einige Verfahren sind Datenschutz-Folgenabschätzungen zwingend vorgeschrieben, definiert über sogenannte „Black-Lists“. Im Rahmen des Prozesses müssen die Verfahren beschrieben, Risiken identifiziert und dann überprüft werden, ob getroffene Schutzmaßnahmen die Risiken angemessen behandeln. Doch Vorsicht – auch wenn die Angemessenheit im Auge des Betrachters liegt, sorgen Sie stets dafür, dass Sie entsprechendes Know-How zu Rate ziehen. Denn Maßnahmen, welche im Falle des Falles als nicht angemessen durch die Behörden betrachtet werden, bergen ein hohes Risiko auf eventuelle Schadensersatzansprüche oder Bußgeldverfahren. Prüfen Sie also, ob Ihre Lösungen dem Stand der Technik entsprechend und den Risiken gegenüber ausreichend sind.

Kleiner Tipp: Auch wenn Sie nicht zu einer Datenschutz-Folgenabschätzung verpflichtet sind, weil die Risiken auf die personenbezogenen Daten keine erforderlich machen, so nutzen Sie trotzdem den risikobasierenden Ansatz, um Gefahren für Ihren Unternehmenserfolg zu adressieren und geeignete Maßnahmen zu treffen. Denn auch hier gilt, Vorsicht ist besser als Nachsicht.

Weitere Informationen gewünscht?

Management Summary Microsoft 365 (kostenlos) und Cloud-Computing sowie ein 80-seitiger Praxisleitfaden Microsoft 365 und Datenschutz sind auf Anfrage unter info@althammer-kill.de direkt bei den Autoren erhältlich.

Checkliste

Das müssen Sie bei Einführung von Microsoft 365 und anderen Cloud-Lösungen beachten:

Heutige Strukturen analysieren und Zielkonzept erarbeiten

- ✔ Lizenzmodell und zu nutzende Dienste identifizieren
- ✔ Bestandsaufnahme zu heutigen Systemen und Datenflüssen durchführen
- ✔ Vertragliche Fragen und Rechtsgrundlagen klären (Gemeinsame Verantwortung/Auftragsverarbeitung, Interessensabwägung formulieren)

Datenschutz-Folgenabschätzung durchführen

- ✔ Datenschutzkonzept erstellen, Verfahren dokumentieren
- ✔ Risiken identifizieren, analysieren und mit Datenströmen abgleichen
- ✔ Maßnahmen ergreifen, um Datenschutzkonformität zu erreichen

Berechtigungen, Schutzmaßnahmen und Wirksamkeit implementieren

- ✔ Betrachtung möglicher Konfiguration/Gruppenrichtlinien
- ✔ Technische und organisatorische Maßnahme implementieren
- ✔ Restrisiko ermitteln und Datenschutz-Folgenabschätzung ergänzen

Gesamtkonfiguration regelmäßig kritisch überprüfen

- ✔ IT-Sicherheitsanalyse der Konfiguration vornehmen
- ✔ Laufende Anpassung an technische und rechtliche Weiterentwicklung
- ✔ Regelmäßige Kontrolle auf Wirksamkeit durch Penetrationstests