Digitalisierung und Datenschutz: So gelingt die Cloud-Migration

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

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:

- 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. Office 365 stellt dabei einen der wohl bekanntesten Service dar. Aber auch Projekttools wie Atlassian Jira, ganze ERP-Lösungen und weitere unternehmensunterstützende Software lässt sich aus der Wolke beziehen. Hier genießen Sie als 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 Unter-nehmer 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

Allen 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

Besonderen 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 bereitgestellten Geräten thematisieren. Übrigens:

THOMAS ALTHAMMER
Althammer & Kill GmbH & Co. KG
Hannover

GESCHÄFTSFÜHRER, MITBEGRÜNDER, BERATER

Thomas Althammer ist studierter Wirtschaftsinformatiker. Zusammen mit seinem 30-köpfigen Team berät er Träger und Einrichtungen im Bundesgebiet zu den Themen Datenschutz, Informationssicherheit und IT-Compliance. Neben seiner Tätigkeit als Geschäftsführer von Althammer & Kill ist er als Lehrbeauftragter an der Fachhochschule der Diakonie in Bielefeld und an der Kath. Universität Eichstätt-Ingolstadt aktiv.

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 integre 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 Veränderungen Ihrer Informationen protokollieren, nachvollziehbar machen und böswillige Veränderungen verhindern. Besonderer 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 „Blacklists“. Im Rahmen des Prozesses müssen die Verfahren beschrieben, Risiken identifiziert und dann überprüft werden, ob getroffenen 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!

Jeder Dienst ist so einzigartig wie Ihr Unternehmen und je nach dem, mit welchen Anforderungen Sie Clouddienste nutzen, so steigen auch die Anforderungen an den Datenschutz.

CHECKLISTE: DAS MÜSSEN SIE BEI EINFÜHRUNG VON OFFICE 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

MATTHIAS NIEDUNG
Althammer & Kill GmbH & Co. KG
Hannover

BERATER FÜR INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Matthias Niedung ist Spezialist im Bereich Informationssicherheit. Neben der Zertifizierung als Fachkraft für Datenschutz, ist er sowohl zertifizierter BSI-Grundschutz-Praktiker als auch Information Security Officer nach ISO 27001. Zudem besitzt er die Zertifizierung als Auditor nach ISO 19011. Matthias Niedung verantwortet zudem bei Althammer & Kill den Bereich der IT-Sicherheitsanalysen.

Foto: Adobe Stock/j-mel