anaptis
A PART OF INFOSIM GROUP

Cloud-Lösung von Microsoft – Wie sicher ist sie wirklich?

10 Gründe für die Sicherheit der Microsoft Cloud

anaptis GmbH
Johann-Krane-Weg 36
48149 Münster

t +49 (0) 251 91 79 96 – 0
f +49 (0) 251 91 79 96 – 10
i www.anaptis.com
e info@anaptis.com

Amtsgericht Münster
HRB 9802
USt.-Id Nr. DE814200922

Geschäftsführung:
Markus Rautenberg
Markus Thyen

Inhaltsverzeichnis

Einleitung

Deutschland und die Digitalisierung – eine Hassliebe?! Einerseits lieben wir Deutschen die Forschung sowie Innovationen, andererseits werden neue Technologien vor dem Einsatz genauestens hinterfragt und kritisiert. So ist es auch mit dem Cloud-Computing.

Nichtsdestotrotz deutet der aktuelle Trend nach dem Ergebnis einer Umfrage des Branchenverbands bitkom auf einen zunehmenden Einsatz von Cloud-Lösungen in Deutschland hin. Die Nutzung von Cloud-Lösungen ist seit einigen Jahren auf Wachstumskurs, was darauf schließen lässt, dass Unternehmen ihre eigene Digitalisierung vorantreiben – natürlich immer unter Beachtung der europäischen und deutschen Sicherheitsvorschriften.

Nach der bitkom-Umfrage nutzen drei von vier Unternehmen heute bereits die Cloud (76 % der Befragten). Dabei ist die Private Cloud* stärker vertreten (58 % der Befragten) als die Public Cloud** (38 % der Befragten). Der geringe Anteil der Public Cloud Nutzer geht auf Sicherheitsbedenken der Befragten zurück. Schließlich befürchten 7 von 10 Befragten unberechtigte Zugriffe auf sensible Unternehmensdaten. Außerdem ist die Rechtslage für einige Befragte unklar und wieder andere argumentieren mit einer schwierigen Integration in bestehende Netzwerke. Völlig unbegründet, wie sich in diesem Whitepaper noch herausstellen wird. Wenn Sie bislang schon überzeugt waren, aber Ihre IT-Entscheider oder die Geschäftsführung die Cloud aus Sicherheits- und Compliance-Gründen nicht nutzen wollten, sollte mithilfe dieses Whitepapers jede Sorge aus dem Weg geräumt sein. Gleiches gilt für den Fall, dass Sie selbst noch skeprisch sind.

Wo wir beim Thema sind – dieses Whitepaper ist u. a. für folgende Personen gedacht:

- überzeugte Microsoft-Cloud-Verfechter, die Dritte überzeugen möchten
- Skeptiker, die noch Zweifel an der Cloud-Lösung von Microsoft haben

Ein Fakt, über den Sie sich vielleicht noch nicht bewusst waren, nehmen wir vorweg: Sie können künftig entscheiden, ob Sie die europäischen Rechenzentren oder sogar die Rechenzentren in Deutschland nutzen möchten. Ihrem Einstieg in die Cloud steht aus unserer Sicht spätestens seitdem nichts mehr im Wege. Dies gilt auch für Branchen mit sensiblen Kundendaten. Überzeugen Sie sich selbst!

*Private Cloud: Bei der Private Cloud handelt es sich um eine Cloud mit einer exklusiven Infrastruktur zur ausschließlichen Nutzung durch den Eigentümer im eigenen Rechenzentrum.

**Public Cloud: Die Public Cloud stellt Anwendungen und Dienste auf einer gemeinsamen Plattform bereit.

1 Datenschutz und -sicherheit gegen Cyberkriminalität

1.1 Herausforderung und Notwendigkeit für KMU

Gibt man bei Google “Ist die Cl…” ein, wird häufig als erster Vorschlag “Ist die Cloud sicher?” als Suchbegriff vorgeschlagen. Dies verrät, wie viele Leute sich mit der Thematik beschäftigen.

Die Aspekte Datenschutz und Datensicherheit spielen bei der Wahl der Cloud-Lösung eine entscheidende Rolle. So legen Nutzer bei der Wahl einer Software besonders auf die nachfolgenden Kriterien Wert:

- Konformität mit der DSGVO
- transparente Sicherheitsarchitektur
- Möglichkeit der Verschlüsselung der Datenübertragung
- Wahl des Datenspeicherorts
- Rechenzentrum im Rechtsgebiet der EU

Um noch einmal auf die gegoogelte Frage zurückzukommen: Nach den Experten von Microsoft sollte die Frage wohl eher lauten “Wie kann ich meine IT-Infrastruktur so sicher machen, wie es ein großer Cloud-Betreiber kann?”. Gemäß Microsoft kann in puncto Sicherheit kein mittelständisches Unternehmen das Sicherheitslevel erreichen, welches ein Cloud-Betreiber mithilfe seiner Ressourcen bieten kann. An dieser Stelle sind die Ressourcen und das Kapital einfach nicht vergleichbar. Der Schutz bei diesen großen Anbietern geht sogar deutlich über den Standard und vor allem über das hinaus, was KMU in Eigenleistung beispielsweise an Sicherheitskonzepten oder Zugangskontrollen leisten könnten. Zudem investiert Microsoft laufend in die Abwehr von Cyberkriminalität sowie externer Bedrohungen.

Sie dürfen sich Hacker heutzutage nicht mehr nur als Einzelgänger vorstellen, die im Keller sitzen und ein paar Daten stehlen möchten. Cyberkriminalität ist mittlerweile ein ganzer Industriezweig, der aktiv Geld verdient und ist so in den letzten Jahren zu einer großen Herausforderung für Organisationen jeder Branche und Größe geworden. Allerdings spitzt sich das Problem noch mehr zu, wenn man bedenkt, dass KMU mehr als jemals zuvor im Visier von Hackern stehen. Warum? So haben die Hacker ein leichtes Spiel. Das Internet, vernetzte mobile Endgeräte und die steigende Anzahl von Clouddiensten bieten Cyberkriminellen ein breites Betätigungsfeld, um sich Zugang zu sensiblen Informationen und

Interna zu verschaffen oder Abläufe durch Netzwerkangriffe zu sabotieren. Gerade bei kleinen und mittelständischen Unternehmen ist es häufig sehr einfach, Sicherheitslücken aufzuspüren. In großen Unternehmen sind die Sicherheitsvorkehrungen dagegen meist so hoch, dass es ein zu großer Aufwand wäre, diese anzugreifen.

1.2 Höchste Sicherheitsstandards von Microsoft

Aus dem vorangegangenen Kapitel haben wir mitgenommen, dass Cloud-Anbieter eine breite Verteidigungslinie gegen Cyberangriffe etablieren müssen – einerseits gestützt durch umfassende Einblicke in aktuelle Bedrohungsszenarien und andererseits ausgerüstet mit den richtigen Werkzeugen, um kriminelle Aktivitäten zu erkennen, zu unterbinden und abzuwehren.

Aus Sicht von Microsoft sind die Aspekte Datenschutz und -sicherheit untrennbar miteinander verbunden. Mit dem Erwerb einer Microsoft-Lösung sorgen Sie dafür, dass Ihre Daten in der Microsoft Cloud vertraulich bleiben und dauerhaft geschützt werden. Schließlich kennen große Cloud-Anbieter wie Microsoft die Tricks und Vorgehensweisen Krimineller und machen sich dies zunutze, indem Sie in speziellen Abteilungen Daten über Cyber-Angriffe sammeln und damit die Cloud stetig verbessern.

Microsoft verspricht Ihnen in dem Zusammenhang Folgendes:

- kein unautorisierter Zugriff auf Ihre Daten
- Eigentümer Ihrer Daten sind Sie (und nur Sie)
- Verschlüsselung, Datenschutz, Datensicherheit, Compliance
- keine Nutzung Ihrer Kundendaten zu Werbezwecken
- Unterstützung für die Einhaltung der DSGVO

Microsoft verpflichtet sich vertraglich, die Privatsphäre seiner Kunden zu schützen. Zu diesem Zweck bieten Sie Kunden Kontrolle über ihre Daten und Transparenz.

1.2.1 Expertenteams

Microsoft hat sich einen ganzheitlichen Sicherheitsansatz für die Microsoft Cloud auf die Fahne geschrieben, bei dem verschiedene Expertenteams Hand in Hand arbeiten.

Zusätzlich zu den intelligenten Sicherheitssystemen und -tools betreibt Microsoft das *Threat Intelligence Center*, in dem ein Team weltweit Daten überwacht, die auf neue Cyberattacken hinweisen können. Wird eine mögliche Bedrohung entdeckt, gibt das Team die

Informationen an das *Cyber Defense Operations Center (CDOC)* weiter. Hier sitzen Security-Experten, die mögliche Sicherheitsprobleme identifizieren und Kunden informieren, die infiziert oder angegriffen werden könnten.

Ein weiteres Team gehört zur *Digital Crimes Unit (DCU)*. Die Ingenieure und Anwälte arbeiten direkt mit Ermittlern aus der ganzen Welt zusammen, um großangelegte Cyberangriffe und -kriminelle dingfest zu machen. Hier werden pro Tag über 600 Millionen Sicherheitsrisiken erfasst, gespeichert und ausgewertet, um die logische Sicherheit in der digitalen Welt zu erhöhen. Aus unterschiedlichen Workloads, Apps und Plattformen werden laufend Informationen und Einblicke gewonnen, miteinander kombiniert und auf intelligente Weise ausgewertet. So können wir Probleme frühzeitig erkennen und beheben, bevor sie die Geschäftstätigkeit bei unseren Cloudkunden beeinträchtigen, und auch die Verfügbarkeit von Apps und Daten wird durchgängig sichergestellt.

1.2.2 Automatische Sicherheitsupdates

Sie als Kunde profitieren auch davon, dass Updates automatisch durchgeführt werden und Sie somit immer auf dem aktuellen Sicherheitsstand sind (Bezeichnung: Evergreening). Die Bereitstellung von Updates erfolgt global, sobald beispielsweise Lücken oder Bedrohungen bekannt werden.

Die Vorteile für Sie als Nutzer – speziell in Abgrenzung zur klassischen Inhouse-Installation von Software und Systemen – liegen auf der Hand:

- Arbeiten mit der sichersten, aktuellen Version Ihrer Cloudlösung zu jeder Zeit
- kein Migrationsaufwand/keine Lizenzgebühren, da alle Kosten bereits in Ihren laufenden Abonnementsgebühren enthalten sind
- keine Reservierung von IT-Ressourcen für die laufende Wartung und Upgrades oder für die Bereitstellung und Einführung zusätzlicher Funktionen

2 Transparenz und Investitionsschutz

Microsoft hat sich dazu verpflichtet, offen mit seinen Kunden zu kommunizieren und diese laufend zu informieren. Bei Microsoft erhalten Sie detaillierte Einblicke in die Maßnahmen, die rund um die Onlinedienste ergriffen werden, um einen reibungslosen Betrieb und den Schutz der Daten zu gewährleisten. Beispielsweise darüber, …

- … wie Ihre Daten verwaltet werden und wo sie sich befinden.
- … wie auf Zugriffsanforderungen seitens Regierungs- und Justizbehörden reagiert wird.
- … wie Entwicklungspläne für die Microsoft-Clouddienste (Status und Roadmap) aussehen.

2.1 Auskunft über Datenspeicherung

Sie als Kunde erhalten konkrete Informationen und verbindliche Dokumentationen dazu, in welchen Rechenzentren Ihre Kundendaten gespeichert werden. Dabei werden Sie auch über die Einhaltung von internationalen, länderbezogenen und branchenspezifischen Compliance-Standards informiert.

2.2 Auskunft über Datenzugriff

Außerdem erfahren Sie, wer unter welchen Umständen auf die Daten zugreifen kann. Ihnen wird garantiert, dass Daten nicht mit den Daten anderer Organisationen vermischt oder kombiniert werden.

Microsoft gibt Dritten (einschließlich Justizbehörden, anderen Regierungsbehörden oder Zivilprozessführern) keinen direkten oder ungehinderten Zugriff auf Kundendaten – es sei denn, Sie als Kunde selbst haben dazu ausdrücklich eingewilligt.

2.3 Auskunft über Statushistorien, Roadmaps und Preise

2.3.1 Statushistorien

Die im letzten Punkt angesprochenen Statushistorien und Verfügbarkeitsinformationen zu Microsoft Azure sind frei im Internet zugänglich.

2.3.2 Roadmaps

Ebenso transparent werden Kunden und Interessenten mit öffentlich verfügbaren Roadmaps (kurz-, mittel- und langfristig) über die geplanten Weiterentwicklungen der

Microsoft-Clouddienste informiert. Die Roadmaps veranschaulichen, an welchen Neuerungen und Verbesserungen derzeit gearbeitet wird, welche Entwicklungsvorhaben auf der Agenda stehen und welche Funktionen in den vergangenen Monaten eingeführt worden sind. Damit ist Microsoft einer der wenigen Anbieter weltweit, der seine Produktpläne mit langfristiger Perspektive einer breiten Öffentlichkeit zur Verfügung stellt.

2.3.3 Preisstabilität

Microsoft hat sich nicht nur zu Transparenz und Offenheit verpflichtet, sondern bietet Kunden und Anwendern auch eine nachhaltige Preisstabilität und einen überzeugenden Return on Investment.

Um Ihnen die Abschätzung der Kosten für Ihre Cloudinfrastruktur zu erleichtern, gibt es beispielsweise für Azure einen Preisrechner, um die erforderlichen Aufwendungen je Dienst zu berechnen und einen Gesamtkostenrechner, mit dem Sie die Total Cost of Ownership kalkulieren können. Bei den Microsoft-Clouddiensten profitieren Sie stets von einer transparenten Preisgestaltung pro Benutzer und Monat sowie von einer unkomplizierten Abrechnung. Sie bezahlen nur für das, was Sie auch tatsächlich nutzen – ohne böse Überraschungen.

Die Vorteile für Sie als Kunde liegen auf der Hand:

- langfristige Planungssicherheit und Preisstabilität
- Schutz für bereits getätigte und neue Investitionen
- öffentlich verfügbare Roadmaps: Einblicke in die Planung für die Microsoft-Clouddienste
- Branchenweit führendes, finanziell abgesichertes SLA mit 99,9-prozentiger Verfügbarkeitszusage
- Cloud als Fokusthema bei Microsoft: 15 Mrd. US-Dollar in Cloud-Infrastruktur investiert

3 IOS-Standards und Zertifikate

Microsoft bietet ein breites Compliance- und Zertifizierungsportfolio, das branchenweit einzigartig ist.

Seit Herbst 2019 werden die Cloud-Lösungen von Microsoft aus zwei deutschen Rechenzentren bereitgestellt, die den Schwerpunkt der künftigen Cloud-Strategie von Microsoft Cloud Deutschland ausmachen werden. Seitdem können Microsoft Partner, wie wir es sind, folglich Lösungen wie Microsoft Azure, Microsoft Office 365 sowie Microsoft Dynamics 365 im vollen Funktionsumfang aus deutschen Rechenzentren bereitstellen. Dabei erfolgt die Speicherung der Kundendaten in einem Data Center in Frankfurt. Das zweite Rechenzentrum in Berlin ist für die Replikation vorgesehen, um eine dauerhafte Ausfallsicherheit zu gewährleisten.

Die Microsoft Cloud erfüllt auf diese Weise

- nationale (z. B. C5-Testat des BSI-Anforderungskatalogs),
- europäische (z. B. EU-DSGVO),
- internationale sowie
- branchenspezifische

Compliance-Standards, Gesetze und Richtlinien, die für Clouddienste in Bezug auf Datensicherheit und Datenschutz gelten. Diese Kompetenz lässt Microsoft sich regelmäßig durch Dritte bestätigen – so werden regelmäßig aktuelle Prüfberichte, beispielsweise zu den ISO-Standards wie ISO 27001, offengelegt. Speziell in Deutschland wird das Versprechen regelmäßig durch deutsche Datentreuhänder kontrolliert. Beispiele für weitere Richtlinien, die eingehalten werden:

- Information technology – Security techniques – Information security management systems (ISO 27001)
- Code of Practice for Protecting Personal Data in the Cloud (ISO 27018)
- FedRAM (Federal Risk and Authorization Management Program)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability (HIPAA/HITECH)
- Service Organization Controls (SOC 1 und SOC 2 Typ 2-Berichte)

4 Sichere Rechenzentren

Microsoft betreibt seine 200 Onlinedienste in 100 internationalen Rechenzentren in 40 Ländern weltweit. Mit jährlichen Investitionen von 6 Mrd. US-Dollar in die Verbesserung der Cloud-Infrastruktur liegt Microsoft branchenweit an der Spitze. Die Rechenzentren sorgen rund um die Uhr dafür, dass Sie geräte-, standort- sowie zeitunabhängig arbeiten können. Zudem haben Sie als Kunde die Entscheidungsfreiheit bei der Wahl des Rechenzentrums.

Die Absicherung der Microsoft Rechenzentren bietet in der Regel einen effektiveren Schutz als die Maßnahmen, die Sie als Kunde selbst für Ihre On-Premise-IT realisieren könnten und lässt sich in jedem Rechenzentrum auf vier Ebenen runterbrechen:

- Gebäudesicherung (Kapitel 4.1)
- Zugangskontrollen (Kapitel 4.1)
- Hardwareschutz (Kapitel 4.1)
- Perimeterabsicherung (Kapitel 4.2)

4.1 Gebäudesicherung, Zugangskontrollen und Hardwareschutz

Physisch werden die Rechenzentren durch ein Mehr-Schicht-Prinzip abgesichert, sodass Sie als Kunde von einer Rechenzentrumsredundanz in jeder Region profitieren. Dazu zählen beispielsweise die folgenden Maßnahmen:

- Zäune
- Bewegungssensoren
- Videoüberwachung
- Alarmanlagen über eine rollenbasierte Zugriffssteuerung für autorisierte Personen
- Georedundanz
- Notfallwiederherstellung

4.2 Perimeterabsicherung

Die Infrastruktur der Rechenzentren wird kontinuierlich überwacht, mithilfe von Penetrationstests geprüft und dazu laufend optimiert, um eine durchgängig hohe Leistung der Sicherheitskontrollen und -prozesse im Rechenzentrum zu gewährleisten. Gegenwärtig erreicht Microsoft durch diese Maßnahmen eine Ausfallsicherheit von 99,98 % und damit einen nahezu unterbrechungsfreien Betrieb der Microsoft-Clouddienste.

5 Rechtssicherheit

Microsoft investiert pro Jahr über eine Milliarde US-Dollar, um die Sicherheit der Daten von Kunden und der eigenen Systeme zu gewährleisten. Denn nur wenn die Nutzer Vertrauen in Technologien haben, kann Fortschritt entstehen.

5.1 Verträge

Microsoft bietet ein Vertragswerk mit Zusicherungen bezüglich internationaler und nationaler Datenschutzgesetze. Sie als Kunde sind damit rechtssicher unterwegs und erhalten eine Bestätigung zur rechtskonformen Nutzung von Onlinediensten (z. B. Auftragsdatenverarbeitungsvereinbarung (ADV) und Zeichnung der EU-Standardvertragsklauseln (EU Model Clauses) für deutsche Unternehmen).

5.2 Sicherheitsverstöße

Bei Sicherheitsverstößen geht Microsoft strukturiert über interne sowie externe Teams vor und ahndet sicherheitsrelevante Angriffe. Die Angreifer werden ermittelt sowie seitens Microsofts zivil- und strafrechtlich belangt. Gleichzeitig informiert Microsoft seine Kunden proaktiv bei derartigen Vorfällen und stellt geeignete Werkzeuge bereit, um die Folgen eines Angriffs einzudämmen und einen potenziellen Schaden möglichst gering zu halten.

Wie geht’s jetzt weiter?

Alle Cloudtechnologien und -dienste von Microsoft sind von Grund auf für den professionellen Einsatz in Organisationen jeder Größe und Branche konzipiert worden. Sie sind nicht nur sicher und Compliance-konform, sondern dank laufender Cloud-Updates auch immer auf dem neuesten Stand – Stichwort Evergreening. Dies macht sich insbesondere bei neuen Sicherheitsfunktionen bezahlt, da eventuelle Lücken rasch geschlossen werden können, bevor Angreifer sie ausnutzen. Dabei durchlaufen alle Updates mehrere Phasen interner Validierungen und Qualitätsprüfungen, bevor sie freigegeben werden.

Das waren sicherlich eine Menge Informationen. Jetzt liegt es an Ihnen, wie es weitergehen soll. Wir können Ihnen Folgendes anbieten:

- Testversion für Dynamics 365 Business Central
- Live-Demo für Dynamics 365 Business Central
- Beratungsgespräch

Testen Sie selbst alle Funktionen oder lassen Sie sich einen Einblick durch unsere Experten geben. Alternativ beraten wir Sie gerne umfassend und beantworten all‘ Ihre Fragen rund um die ERP-Software. Vereinbaren Sie einfach einen Termin mit einem unserer Experten.

Tel. 0251 / 91 79 96 - 0

E-Mail info@anaptis.com