Cloud – Sind meine Daten bei Microsoft auch geschützt?

Die Produkte von Microsoft sind sehr beliebt – sei es Office 365, SharePoint oder Teams. Doch auch weitere Tools wie der OneDrive oder Sway werden immer intensiver genutzt. Da ist es wichtig, sich auch mit dem Datenschutz auseinanderzusetzen.

Bild 1: Datenspeicherort.

Microsoft ist hier sehr offen und stellt viele Informationen dazu zur Verfügung. Zeit für eine Übersicht.

Datenhaltung

Teams

Im Admin-Center kann angezeigt werden, in welchem Rechenzentrum die Daten liegen (Settings –> Organization profile –> Data location. Dies sieht beispielsweise wie im Bild 1 aus.

Da Microsoft auch Rechenzentren in der Schweiz betreibt, sollten die Daten in diese migriert werden. Die beiden Serverräume stehen in Zürich und Genf, genügen also auch den BSI-Anforderungen. Diese sagen aus, dass das Backup-Rechenzentrum mindestens 200 km vom Haupt-standort entfernt sein muss.

Wichtig bei Teams ist aber auch, wo welche Daten abgelegt werden (Bild 2).

Die Daten eines konfigurierten Teams werden in einer Microsoft 365 Gruppe und ihrer SharePoint-Webseite inkl. Exchange-Mailbox gespeichert. Private Chats (einschliesslich Gruppen-Chats), Nachrichten, die als Teil einer Konversation in einem Kanal gesendet werden sowie die Struktur von Teams und Kanälen werden in einem Chat-Dienst gespeichert, der in Azure läuft. Die Daten werden auch in einem verborgenen Ordner in den Benutzer- und Gruppenpostfächern gespeichert, um die Informationen vor einem Verlust zu schützen.

Sprachnachrichten werden in Exchange gespeichert. Kontakte werden im Exchange-basierten Cloud-Datenspeicher abgelegt. Exchange und der Exchange-basierte Cloud-Store werden im gebuchten Rechenzentrum abgelegt.

Medien, die in Chats verwendet werden (mit Ausnahme von Giphy GIFs, die nicht gespeichert werden, sondern nur einen Verweis auf die ursprüngliche URL des Giphy-Dienstes erhalten), werden in einem Azure-basierten Mediendienst gespeichert, der an denselben Orten wie der Chat-Dienst steht.

Dateien (einschliesslich OneNote und Wiki), die jemand in einem Kanal gemeinsam nutzt, werden auf der SharePoint-Website des Teams gespeichert. Dateien, die in einem privaten Chat oder in einem Chat während einer Besprechung oder eines Anrufs freigegeben werden, werden hochgeladen und im OneDrive des Geschäftskontos des Benutzers, der die Datei freigibt, gespeichert. Exchange, SharePoint und OneDrive werden ebenfalls im gebuchten Rechenzentrum gespeichert.

Wichtig: werden zusätzliche Plugins genutzt, werden die Daten auch dort gespeichert. So zum Beispiel bei der Benutzung von Dropbox, LinkedIn oder ähnlichen. Somit verlassen solche Dienste ziemlich sicher den EU-Raum und es ist grosse Vorsicht geboten.

Office Dienste

Wenn das Schweizer Rechenzentrum ausgewählt wird, werden die verschiedenen Daten an folgenden Orten gespeichert:

- Exchange Online –> Schweiz
- OneDrive for Business –> Schweiz
- SharePoint Online –> Schweiz
- Skype for Business –> EMEA
- Microsoft Teams –> Schweiz
- Office Online & Mobile –> Schweiz
- EOP –> Schweiz
- Intune –> EMEA
- MyAnalytics –> Schweiz
- Planner –> EMEA
- Sway –> Vereinigte Staaten
- Yammer –> EMEA
- OneNote Services –> Schweiz
- Stream –> EMEA
- Whiteboard –> EMEA
- Formulare –> EMEA
- Workplace Analytics –> Vereinigte Staaten

Es ist ersichtlich, dass nur Daten von Sway und Workplace Analytics in den USA gespeichert werden. Alle anderen sind entweder in der Schweiz oder in der EU vorhanden. Gemäss Aussage von Microsoft werden die Ana-

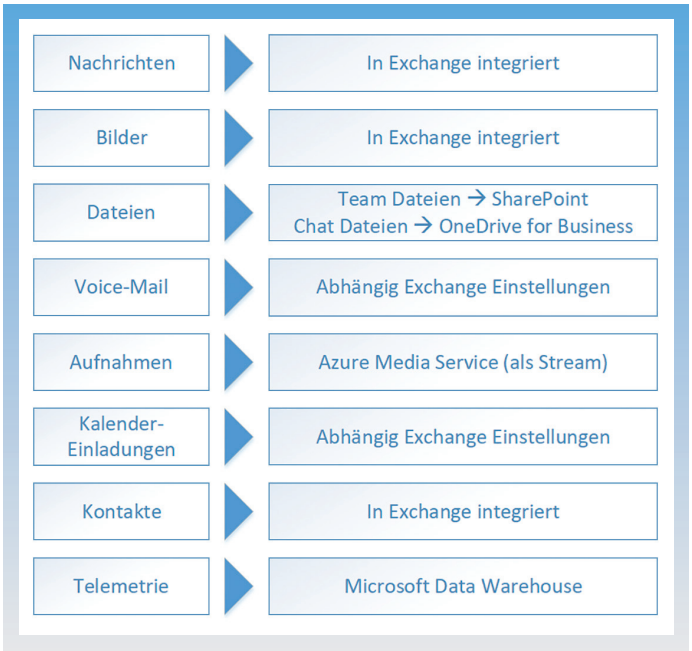

Bild 2: Teams-Daten.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Bild 3: Verschlüsselte Text-Datei.

lytics Daten aus dem gesamten EU-Raum anonymisiert und können damit nicht auf eine einzelne Person zurückverfolgt werden.

Zertifizierungen

Microsoft verfügt über praktisch alle wichtigen Zertifizierungen im IT-Sicherheitsbereich. Dazu gehören unter anderem die ISO 27001 (Anforderungen an ein Informationssicherheitsmanagementsystems ISMS), ISO 27018 (Verhaltenskodex zum Schutz von personenbezogenen Daten in der Cloud), die neue ISO 27701 (Datenschutz-Informationsmanagementsystem) oder die SOC 1, 2, und 3 (Service Organization Controls). Viele weitere, auch Regionale sind mit dabei. Eine komplette Übersicht ist unter https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home?view=o365-worldwide zu finden.

Herausforderungen

Immer wieder ist davon zu hören, dass Microsoft ja ein amerikanisches Unternehmen ist und entsprechend diese Gesetze gültig sind. Gerade die Herausgabe von Daten gibt immer wieder Stoff zu Diskussionen. Microsoft nimmt dazu wie folgt Stellung: «Für den Fall, dass Microsoft einen Auftrag zur Offenlegung von Daten erhält, wird Microsoft keine Daten an die Behörden aushändigen, sondern wird die ersuchende Behörde direkt an den Kunden verweisen. Sollte jedoch die Behörde immer noch von Microsoft die Offenlegung von Daten verlangen, wird Microsoft den Antrag auf Offenlegung umfassend aus rechtlicher Sicht prüfen.»

Somit bleibt ein Restrisiko bestehen. Jedoch ist der Kunde «gewarnt», dass ein entsprechendes Vorgehen der amerikanischen Behörden am Laufen ist.

Unter www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report zeigt Microsoft, wie viele Fragen an ihr Unternehmen gestellt wurden. So sind im zweiten Halbjahr 2019 240 Anfragen von Behörden zu 319 Benutzern gestellt worden. 19 Prozent der Anfragen wurden von Microsoft abgelehnt. Bei 43 Prozent wurden nur Metadaten wie E-Mail-Adresse, Land, IP-Adresse, Xbox-Gamertag, Kreditkarten-Informationen oder Rechnungsdaten zugestellt. Bei 38 Prozent wurden keine zur Anfrage passenden Daten gefunden.

Können nun Daten in der Cloud abgelegt werden? Sensible Daten dürfen nicht ohne zusätzliche Sicherheitsvorkehrungen innerhalb einer Cloud-Anwendung wie beispielsweise SharePoint Online gespeichert werden. Hierzu müssen die Anforderungen zum Thema Datenverschlüsselung erfüllt werden. Neben einer zusätzlichen Verschlüsselung (Zum Beispiel auf Basis von Azure Information Protection) werden sowohl in den Rechenzentren als auch der eingehende und ausgehende Datenverkehr verschlüsselt. Eine Möglichkeit ist nun, nicht auf Personen bezogenen Daten in der Cloud abzulegen, alle weiteren sollten jedoch auf eigenen Servern liegen.

Aber sind die Daten denn wenigstens sicher? Wenn man alle die Zertifizierungen und Bemühungen von Microsoft anschaut: Ja, auf jeden Fall. Gerade was die technische und physische Sicherheit anbetrifft, wird alles unternommen. Microsoft gewährt einen kleinen Einblick in die Cloud. Nach einer kurzen Registrierung unter https://resources.office.com/ww-modern-workplace-webinar-mwep106-registration-on-demand.html können Video-Bilder von einem der verschiedenen Rechenzentren bestaunt werden. Brad Smith, President und Chief Legal Officer sagt dazu ganz klar: «Wenn wir unsere Kunden nicht schützen können, haben wir ihr Vertrauen nicht verdient.» So kann selbst Microsoft nicht einfach auf die Daten ihrer Kunden zugreifen. Alle Server sind physisch verschlossen. Kommt es zu einem Support-Vorfall und ein Microsoft-Mitarbeiter muss an die Hardware ran, wird ein interner Freigabeprozess durchlaufen. Der jeweilige Manager gibt für eine bestimmte Dauer den Zugriff auf diesen Server frei.

Weitere Schutzmöglichkeiten

Microsoft bietet die Lösung Enterprise Mobility & Security (EMS) an. Diese umfasst die folgenden Dienste:

- Azure Information Protection für Informationsschutz
  - Klassifizierung und Verschlüsselung von Dateien
  - Data Loss Prevention
  - Benutzersensibilisierung durch Benachrichtigungen
- Intune für verwaltete mobile Produktivität
  - Verwaltung mobiler Geräte und Anwendungen
  - Cloud App Security für identitätsorientierte Sicherheit
  - Unternehmensweite Sichtbarkeit, Kontrolle und Schutz für Cloud-Anwendungen
- Azure Active Directory für Identitäts- und Zugriffsverwaltung (IAM)
  - Sicheres Single Sign-on für Anwendungen in der Cloud und lokal
  - Multi-Faktor-Authentifizierung
  - Bedingter Zugriff / Risikobasierte Zugangsberechtigung
  - Erweiterte Sicherheitsberichte
- Advanced Threat Analytics für identitätsorientierte Sicherheit
  - Schutz vor erweiterten und zielgerichteten Angriffen durch Anwendung von Verhaltensanalysen über Anwender und Entität

Die Frage, die sich aber bei allen Möglichkeiten stellt: Möchten wir wirklich auch die Verschlüsselung Microsoft anvertrauen? Falls dies für Sie nicht in Frage kommt, gibt es zum Beispiel mit Boxcryptor eine gute Alternative. Boxcryptor verschlüsselt alle Daten, bevor diese in die Cloud kopiert werden. Seit Mitte Juli 2020 werden auch die Daten von Teams mitberücksichtigt und verschlüsselt. Sollten die Zugangsdaten in falsche Hände gelangen, kann ohne den entsprechenden Schlüssel nichts damit angefangen werden. Eine verschlüsselte Text-Datei sieht beispielsweise wie in Bild 3 aus.

Fazit

Ja, wir können die Daten Microsoft Datenschutz-konform anvertrauen, wenn diese im Schweizer Rechenzentrum liegen. Microsoft unternimmt alles, diese technisch, wie auch physisch zu schützen. Regelmässig erfolgen Audits von akkreditierten Stellen, die dies überprüfen. Entsprechende Berichte legt Microsoft offen und können studiert werden. Ein gewisses Rest-Risiko bleibt bei der aktuellen Rechtslage aber. Daher sollten die Daten zusätzlich selber durch Verschlüsselung geschützt werden. So bleiben diese unter eigener Kontrolle und gelangen auch bei einem erfolgreichen Hackerangriff nicht in falsche Hände. Mit der notwendigen Vorsicht können damit Cloud-Dienste optimal genutzt werden.

Viele weitere infos von Microsoft sind unter den folgenden Links zu finden:

- Datenschutz-News: https://news.microsoft.com/de-de/datenschutz-microsoft/
- Datenschutzerklärung: https://privacy.microsoft.com/de-DE/privacystatement
- Lizenz-Informationen: https://privacy.microsoft.com/de-DE/privacystatement
- Wo werden Daten gespeichert: https://docs.microsoft.com/de-de/office365/enterprise/o365-data-locations