IT-Sicherheitstipp Nr.8 – Oktober 2019

Umgang mit Cloud-Diensten

Was sind Cloud-Dienste?

Das Internet ist für die meisten von uns nur einen Mausklick oder Fingerdruck entfernt, sei es vom Arbeitsplatzrechner, sei es vom Smartphone aus. Die Übertragungsgeschwindigkeiten und die Speichermöglichkeiten im Internet sind mittlerweile so gut, dass bestimmte Angebote direkt im Internet genutzt werden können, ohne sie lokal zu installieren.

Diese Angebote reichen von Speicherplatz für Fotos oder Videos bis hin zur Möglichkeit, Computerprogramme, die im Internet liegen, über den Browser so zu nutzen, als wären sie vor Ort installiert. Die Zahl der Nutzerinnen und Nutzer ist dabei grundsätzlich beliebig.

Auch Verwaltungen nutzen heute bereits Cloud-Dienste!

Heiter bis wolkig
Cloud-Dienste bieten für eine Vielzahl von Personen – oft kostenfrei – die Möglichkeit, über das Internet Daten und Programme zu nutzen. Die damit verbundene hohe Verfügbarkeit wird oft damit erkauft, dass auch die Anbieter der Dienste Zugriff auf die Daten haben.

Überblick über Cloud-Dienste

Zu den typischen Cloud-Diensten zählen u.a.

- Speicher (z.B. für Fotos)
- Anwendungen (z.B. Bildbearbeitungsprogramme)
- Rechenleistungen (z.B. Internet-Server für eine eigene Homepage)

Bei einigen dieser Dienste ist es den Anbietern gleich, für welchen konkreten Zweck sie genutzt werden – die freie Nutzbarkeit ist dann Teil des Geschäftsmodells.

Cloud-Dienste werden sowohl kostenpflichtig als auch kostenfrei angeboten. Bei den kostenfreien Angeboten teilt man sich die Dienste mit Dritten, bei den kostenpflichtigen werden – je nach Vertrag – die erforderlichen Betriebsmittel exklusiv zur Verfügung gestellt.

Begrifflich unterscheidet man entsprechend zwischen:

„Private Cloud" – exklusive Bereitstellung der Betriebsmittel (Speicherplatz, Rechenleistung etc.) für die beauftragende Stelle

„Public (Öffentliche) Cloud" – übergreifende Bereitstellung der Betriebsmittel für jedermann

Deutsche Verwaltungen nutzen regelmäßig „Private Clouds". Über ihre Rechenzentren werden zentrale Dienste wie z.B. E-Mail, aber auch der Betrieb von Web-Servern oder Speicherplatz als „Private Cloud" behördenintern genutzt.

Vorteile von Cloud-Diensten

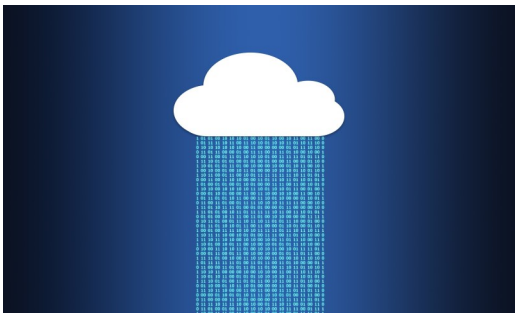
Cloud-Dienste werden oft so angeboten, dass die Kundinnen und Kunden sehr kurzfristig die Dienste in Anspruch nehmen, erweitern oder verringern können. Idealerweise merken die Nutzerinnen und Nutzer nicht, dass z.B. weiterer Speicher wegen verstärkter Nutzung hinzugeschaltet wird, um die Dienste in der versprochenen Qualität anzubieten.

LANDKREIS MARBURG BIEDENKOPF

Projekt der interkommunalen Zusammenarbeit

Cybersicherheit

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR



Die Kundinnen und Kunden müssen nicht selbst Hard- und Software betreiben, die manchmal aufwändig angepasst werden muss. Dies ist besonders von Vorteil, wenn die Nutzung wieder verringert wird. Bei den kostenpflichtigen Cloud-Diensten zahlt man regelmäßig nur für den laufenden Betrieb, der in kurzen Zeitspannen abgerechnet wird – teilweise nach Stunden!

Die Dienste werden in Netzwerken bzw. über das Internet von spezialisierten Anbietern betrieben. Diese betreuen die Hardware und die Software in dafür ausgelegten Rechenzentren – die Nutzerinnen und Nutzer müssen sich darum nicht kümmern.

Gefahren bei Cloud-Diensten

Wenn man Cloud-Dienste nicht auf eigenen Rechnern betreibt, müssen die Daten Dritten anvertraut werden. Während Privatpersonen häufig auf kostenfreie Angebote zurückgreifen, bei denen sie die Dienste mit einer Vielzahl von anderen teilen („Public Cloud“) und die oft im Ausland betrieben werden, nutzen Verwaltungen meistens kostenpflichtige sichere „Private Clouds“.

Cloud-Dienste selbstgemacht
Cloud-Dienste kann man auch selbst zu Hause betreiben. Über kostenfreie Software können auf heimischen Rechnern Speicherplatz, Adressbücher, Kalender etc. für Familie und oder Freunde freigegeben werden.

Sie haben dann solche Nutzungsverträge, bei denen die Datensicherheit und der Zugangsschutz neben der Verfügbarkeit, die für Privatanwender oft im Vordergrund steht, wesentliche Vertragsinhalte sind. Das bedeutet beispielsweise, dass die Server ausschließlich in der EU, besser noch in Deutschland, und dadurch unter entsprechendem Recht, stehen, eine sichere Ende-zu-Ende Verschlüsselung der Daten gewährleistet ist oder eine automatische Datensicherung im Hintergrund läuft.

Andernfalls besteht die Gefahr, dass

- Dritte unberechtigt Zugang zu den Daten haben,
- der Anbieter oder seine Auftragnehmer die Daten für eigene Zwecke nutzen,
- Daten verloren gehen bzw. nicht zeitgerecht verfügbar sind,
- unbemerkt Kopien von Daten durch den Anbieter angelegt und ggf. nicht gelöscht werden.

Mit den richtigen Schutzmaßnahmen kann diesen Gefahren vorgebeugt werden!

Cloud Dienste sicher nutzen

Sie können davon ausgehen, dass Ihre Verwaltung, wenn sie Cloud-Dienste nutzt, die Anbieter und Verfahren sorgfältig ausgewählt hat. Hierbei hat sie Vorgaben formuliert und sich versichert, dass die geschilderten Gefahren beherrschbar sind.

Bedenken Sie, dass oft schon auf Ihrem Smartphone oder Ihrem privaten Computer Cloud-Dienste des Herstellers vorinstalliert sind und Ihre Daten und manchmal auch Ihr Nutzungsverhalten (z.B. Anrufprotokolle) beim Hersteller gespeichert werden!

Dienstliche Daten dürfen selbstverständlich nur im dienstlichen Umfeld und in dienstlich freigegebenen Cloud-Diensten verarbeitet werden, nicht in „Ihrer“ Cloud!

Wer liest mit?
Wissen Sie, wer Ihre persönlichen Daten in Public Clouds nutzt bzw. nutzen darf? Das Kleingedruckte in den Allgemeinen Geschäftsbedingungen kann so manche Überraschung bereiten!

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf
und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Cybersicherheit

Wenn Sie sich privat für die Nutzung von Cloud-Diensten entschieden haben, sollten Sie folgende Sicherheitsmaßnahmen treffen:

- Informieren Sie sich über den Anbieter – verfügt das Rechenzentrum über Sicherheitszertifikate, z.B. nach „BSI IT-Grundschutz“ oder „ISO 27001“?
- Laden sie möglichst nur Daten in die Cloud, die Sie vorher mit einem Verschlüsselungsprogramm verschlüsselt haben. Zum Beispiel die Open Source Software Cryptomator oder Boxcryptor.
- Speichern Sie keine hochsensiblen Daten in der Cloud.
- Verzichten Sie auf Anbieter, denen Sie Nutzungsrechte an Ihren Inhalten einräumen.
- Prüfen Sie die Einstellungen des Dienstes für Ihre Daten.
- Verwenden Sie sichere Passwörter.
- Halten Sie zuhause Kopien vor.
- Vergeben Sie Zugriffsrechte an Dritte mit Bedacht.

Wenn Sie selbst Cloud-Dienste privat nutzen möchten, sollten Sie sich folgende Fragen stellen:

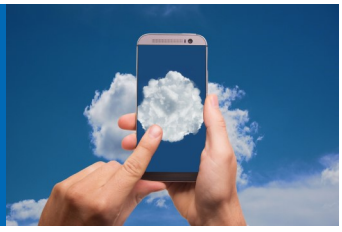
- Welche Daten will ich in die Cloud geben? Urlaubsfotos – oder auch Fotos, die ich nicht allen zeigen würde? Mein Tagebuch oder nur meinen Einkaufszettel?
- Wem will ich die Daten anvertrauen? Einem Unternehmen, das strengen Datenschutzgesetzen unterliegt? Oder einem Unternehmen, das auch Dritten meine Daten offenbart?
- Macht mir der Verlust der Daten etwas aus? Wenn ja, sollte ich zu Hause Kopien behalten.

Was sind Ihre Daten wert?

Wie auch bei Social Media gilt, dass der Preis, den Sie für kostenlose Dienste zahlen, Ihre Daten selbst oder Ihr Nutzungsverhalten ist. Wägen Sie diese gegen (vermeintlich) günstige Angebote ab.

Hinweise:

- Verschlüsseln Sie möglichst Ihre Cloud-Daten!
- Halten Sie Kopien zu Hause vor!
- Im Zweifelsfall: Datei nicht in die Cloud.



Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!