Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cloud-Dienste sicher nutzen

11 Tipps zur sicheren Nutzung von Cloud-Diensten

Tipps rund um Cloud Computing

Ein Cloud-Dienst ist ein Online-Dienst, auf den Sie über das Internet jederzeit zugreifen können – egal, mit welchem Endgerät. Die Daten werden also nicht auf Ihren Geräten gespeichert, sondern in der sogenannten Cloud. So können Sie beispielsweise Dokumente oder Fotos in der Cloud hinterlegen, sie mit anderen teilen oder gemeinsam bearbeiten. Das ist praktisch, birgt aber auch Risiken. Wir haben für Sie Informationen und hilfreiche Tipps rund um Cloud Computing zusammengestellt, die wir Ihnen in dieser Broschüre und auf unserer Website zur Verfügung stellen: bsi.bund.de/cloud-sicherheit

Elf wichtige Tipps, die Sie für eine sichere Nutzung von Cloud-Diensten beherzigen sollten, haben wir hier für Sie zusammengefasst. Ausführliche Informationen dazu finden Sie auf den nachfolgenden Seiten dieser Broschüre.

1. Sorgen Sie für einen ausreichenden Basisschutz Ihres Zugangsgeräts.
2. Sichern Sie den Zugang zu Cloud-Diensten mit einem sicheren Passwort und wenn möglich mit einem zweiten Faktor ab.
3. Auch mobile Geräte, die Apps nutzen, um Zugriff auf Cloud-Dienste zu erhalten, sollten ausreichend gegen Missbrauch abgesichert werden.
4. Prüfen Sie die Datenschutzbestimmungen des jeweiligen Cloud-Anbieters genau, damit Sie wissen, wie Ihre Daten verarbeitet werden.
5. Informieren Sie sich über Haftungsfragen im Falle eines Verlusts Ihrer Daten durch den Anbieter.
6. Überprüfen Sie in den Allgemeinen Geschäftsbedingungen des Anbieters, ob eine Weitergabe Ihrer Daten an Dritte zu kommerziellen Zwecken erfolgen könnte.

7. Informieren Sie sich über die Sicherheitszusagen des Cloud-Anbieters zur Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten, etwa im Falle eines Ausfalls der Rechenzentren.
8. Achten Sie bei der Auswahl Ihres Cloud-Anbieters unbedingt darauf, dass die Übertragung Ihrer Daten über eine sichere Verbindung wie https erfolgt.
9. Wenn Sie persönliche Daten in der Cloud speichern möchten, sollten Sie diese Daten selbstständig verschlüsseln, bevor Sie sie in die Cloud laden.
10. Wenn Sie Daten aus der Cloud mit anderen Personen teilen, achten Sie auf die Art der Freigabe. Begrenzen Sie diese zeitlich und geben Sie nur so viele Daten wie nötig frei.
11. Bevor Sie Ihre Daten einem Cloud-Anbieter anvertrauen, sollten Sie prüfen, wie aufwendig es ist, die Daten wieder aus der Cloud zu entfernen.

Was bedeutet Cloud Computing eigentlich?

Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Der Begriff der Wolke macht zudem deutlich, dass das Innere unbekannt und von außen nicht einsehbar ist. Beim Cloud Computing greifen Sie somit nicht mehr auf die Rechenleistung oder den Speicherplatz Ihres eigenen PCs, Smartphones oder Tablets zurück, sondern nutzen die Rechenleistung eines Cloud-Anbieters. Da die Cloud mit dem Internet verbunden ist, sind Ihre Daten mit unterschiedlichen Endgeräten stets abrufbar. Neben dem Speichern von Daten bieten viele Cloud-Anbieter auch online die Nutzung von Anwendungen an, beispielsweise zum Bearbeiten von Dokumenten.

Wo werden Cloud-Dienste eingesetzt?

Ein beliebter Cloud-Dienst sind Online-Speicher, bei denen Sie Daten hinterlegen und diese von verschiedenen Endgeräten aufrufen oder sie mit anderen Nutzerinnen und Nutzern teilen können. Einige Anbieter ermöglichen es, Ihre Daten auch mit online ausführbaren Anwendungen zu bearbeiten, etwa mit Programmen zur Text oder Grafikbearbeitung. Die Anwendung muss dafür nicht auf Ihrem Rechner installiert sein. Die gespeicherten Dateien können über einen Browser direkt in der Cloud bearbeitet werden.

Ein weiteres Beispiel für einen Cloud-Dienst ist die Web-Mail. Anbieter stellen Ihnen online ein Postfach für Ihre E-Mails zur Verfügung. Die Nachrichten Ihres Online-Postfachs befinden sich dabei auf dem Server des Anbieters. Sie können von jedem Ort aus und mit jedem internetfähigen Gerät auf Ihre E-Mails zugreifen.

Geräte wie Smartwatches oder Fitnesstracker synchronisieren ihre Aufzeichnungen je nach Einstellung mit cloudbasierten Online-Diensten. Diese können die Daten automatisiert nach bestimmten Kriterien auswerten.

Auch die beliebten Video- oder Musik-Streaming-Plattformen sind Cloud-Dienste. Der Anbieter eines Streaming-Dienstes hat über die Analyse des jeweiligen Nutzerverhaltens die Möglichkeit, Auswertungen zu erstellen und so zum Beispiel zielgerichtet Programminhalte oder Werbung einzublenden.

Vorteile der Cloud

Flexibilität und Verfügbarkeit

Der Zugriff auf die in der Cloud gespeicherten Daten ist für Sie jederzeit und von überall mit einem internetfähigen Gerät möglich. Der Cloud-Anbieter ist grundsätzlich für ausreichend Rechenleistung und Speicherplatz verantwortlich. Wie groß diese konkret sind, hängt vom jeweiligen Nutzungsvertrag ab. Oftmals können Sie gegen einen Aufpreis den verfügbaren Speicherplatz erweitern.

Nutzerfreundlichkeit

Cloud-Dienste werden über den Browser oder über Apps aufgerufen. Ohne großen Aufwand können Sie in der Cloud Ihre Daten mit anderen teilen. Dazu müssen Sie die Daten lediglich einmal in die Cloud hochladen. Mit einer entsprechenden Berechtigung können andere dann auf diese zugreifen. Auf diese Weise können Sie eine große Anzahl von Daten oder eine große Datenmenge mit anderen Nutzerinnen und Nutzern teilen.

Aktualität

Software-Anbieter, die ihre Software über die Cloud bereitstellen, halten diese in der Regel auf dem neuesten Stand. Cloud-Nutzerinnen und -Nutzer müssen sich entsprechend nicht um Software-Updates kümmern oder gar eine neue Version erwerben. Sie mieten den Dienst und der Anbieter sorgt für die Bereitstellung der Funktion.

Daten-Backup und Sicherheit

Grundsätzlich ist der Cloud-Anbieter für die Sicherheit der in der Cloud gespeicherten Daten verantwortlich. Regelmäßige Daten-Backups, also das Anlegen einer aktuellen Datensicherung, werden automatisch erstellt. Weitere Sicherheitsaspekte werden ebenso zentral bewerkstelligt, beispielsweise das Einspielen von Sicherheitsupdates für die bereitgestellte Software sowie die Aktualisierung des Virenschutzes. So wird verhindert, dass Angreifer Sicherheitslücken in Software ausnutzen können. Sie sollten allerdings bedenken, dass Sie das nicht aus der Eigenverantwortung nimmt, Ihre Daten ausreichend gut zu schützen.

Als Nutzerin oder Nutzer eines Cloud-Dienstes sollten Sie die Tipps beachten, die wir Ihnen im Folgenden zusammengestellt haben.

1

Basisschutz

Der beste Schutz Ihrer Daten bei einem Cloud-Anbieter nützt wenig, wenn das Gerät, mit dem Sie sich Zugriff auf die Cloud verschaffen, nicht ausreichend geschützt ist. Ein guter Basisschutz ist daher unumgänglich. Schadsoftware auf Ihrem Zugangsgerät kann auch Ihre Daten in der Cloud angreifen. Der Zugriff auf Cloud-Dienste ist oft nur über Benutzername und Passwort geschützt. Sobald jemand anderes diese Zugangsdaten kennt, kann er ungehindert, jederzeit und von überall auf Ihre Daten zugreifen. Der Zugriff über unsichere Netze – etwa ungesicherte WLAN-Hotspots – stellt ein Risiko dar. In diesen Netzen können Angreifer Zugangsdaten mitlesen und missbrauchen (siehe auch Tipp 8).
Weitere Tipps zum Basisschutz erhalten Sie in unserer Broschüre „Das Internet sicher nutzen“ und auf unserer Website bsi.bund.de/internetsicherheit.

2

Zugang zu Cloud-Diensten

Eine einfache Kombination aus Benutzername und sicherem Passwort schützt nicht optimal, denn wenn Dritte über diese Zugangsdaten verfügen, können sie ungehindert auf Ihre Daten zugreifen. Sichern Sie den Zugang zu Ihrem Cloud-Dienst daher zusätzlich ab. Inzwischen bieten immer mehr Cloud-Anbieter eine Zwei-Faktor-Authentisierung an, wie sie beispielsweise beim Onlinebanking eingesetzt wird. Zusätzlich zu Benutzername und einem sicheren Passwort (erster Faktor) wird hier ein weiteres Merkmal eingesetzt, um den rechtmäßigen Nutzer oder die rechtmäßige Nutzerin zweifelsfrei zu authentisieren. Als zweiter Faktor eignet sich beispielsweise eine Hardware-Komponente, die als Schlüssel fungiert.

Das können das Smartphone, eine Chipkarte oder ein spezieller USB-Stick sein. Auch ein Fingerabdruck oder eine vom Anbieter versendete SMS mit einem Einmalcode kann genutzt werden. Auf diese Weise erschweren Sie es Dritten deutlich, sich Zugriff auf den Cloud-Dienst zu verschaffen, da der Diebstahl eines Faktors hierfür nicht ausreicht.

Tipps zu sicheren Passwörtern erhalten Sie auf unserer Website bsi.bund.de/account-schutz.

3

Mobile Endgeräte

Viele Anwender und Anwenderinnen speichern die Zugangsdaten in der App des Cloud-Anbieters auf ihrem Smartphone. Dann genügt ein Aufruf der App, um auf die Daten zuzugreifen. Gelangt das Smartphone in falsche Hände, sind die Daten in der Cloud nur so sicher, wie das Smartphone vor unerlaubtem Zugriff geschützt ist. Sperren Sie Ihr mobiles Gerät daher immer mit einer PIN oder einem biometrischen Merkmal, wie Ihrem Fingerabdruck.

Tipps zum sicheren Umgang mit mobilen Endgeräten erhalten Sie in unserer Broschüre „Smartphone, Tablet und Co sicher nutzen“ und auf unserer Website bsi.bund.de/smartphone-sicherheit.

4

Nutzungsbedingungen und Datenschutzbestimmungen

Jeder Cloud-Anbieter kann seine eigenen Nutzungsbedingungen aufstellen, solange er damit keine Gesetze bricht. Dasselbe gilt für den Datenschutz. Möglicherweise räumen Sie dem Anbieter Zugriffs- und Nutzungsrechte für Ihre gespeicherten Dateien ein, ohne zu wissen, welche das sind. Überprüfen Sie genau, welche Rechte Sie Ihrem Dienstleister einräumen.
Welchen rechtlichen Bestimmungen die in die Cloud übermittelten Daten unterliegen, ist davon abhängig, in welchem Land die Daten tatsächlich in Rechenzentren gespeichert werden. Dies ist für Anwenderinnen und Anwender nicht immer nachvollziehbar. Dadurch können sich die Bestimmungen jedoch von denen in Deutschland oder der EU unterscheiden.

5

Haftungsfragen und Anbieterwechsel

Informieren Sie sich sorgfältig über Haftungsfragen im Falle eines Datenverlustes, einer Anbieterinsolvenz oder eines Eigentümerwechsels. Auch für den Fall eines Anbieterwechsels müssen Sie sich bereits im Vorfeld darüber informieren, ob und wie Sie Ihre Daten aus der Cloud zurückerhalten können.

6

Weitergabe von Daten an Dritte

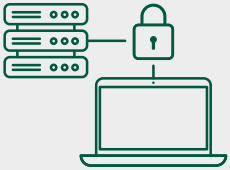
Besonders bei kostenlosen Cloud-Diensten besteht die Möglichkeit, dass der Anbieter Nutzer- oder Nutzungsdaten an Dritte zu kommerziellen Zwecken verkauft oder selbst nutzt. Ein Blick in die Allgemeinen Geschäftsbedingungen (AGB) gibt Auskunft darüber, welche Rechte Sie Ihrem Anbieter einräumen.

7

Vertraulichkeit, Integrität und Verfügbarkeit der Daten

Über verschiedene, durch unabhängige Institutionen vergebene Sicherheitskennzeichen wie Zertifikate und Testate können Sie nachvollziehen, ob ein Cloud-Anbieter festgelegte Sicherheitsstandards erfüllt oder mit den jeweiligen gesetzlichen Regelungen des Staates übereinstimmt. Informieren Sie sich über die Sicherheitszusagen des Cloud-Anbieters. Sind die Daten seitens des Anbieters vor unbefugtem Zugriff geschützt? Kann ihre Unversehrtheit sichergestellt werden? Wie gewährleistet der Anbieter die Verfügbarkeit der Daten? Häufig wird die Verfügbarkeit der Daten im Vertrag mit dem Cloud-Anbieter festgelegt. Ist dort nichts vermerkt, kann es sein, dass nicht immer auf die Daten zugegriffen werden kann.

8



Verschlüsselung der Datenübertragung

Der gesamte Datenverkehr mit der Cloud sollte verschlüsselt erfolgen. Werden die Daten unverschlüsselt übertragen, sind diese für Unbefugte einsehbar, die sich zum Beispiel über einen Man-In-The-Middle-Angriff in Ihre Datenübertragung einklinken. Das bedeutet, dass zwischen Sender und Empfänger die Daten „in der Mitte“ abgegriffen werden. Achten Sie bei der Auswahl Ihres Cloud-Anbieters unbedingt darauf, dass die Übertragung über eine sichere Verbindung wie https erfolgt.

9

Datenverschlüsselung

Wenn Sie die Cloud als Speicherplatz für persönliche Daten nutzen möchten, sollten Sie diese Daten selbstständig verschlüsseln, bevor Sie sie in die Cloud laden. Viele Cloud-Anbieter bieten eine Verschlüsselung der Daten in der Cloud bereits an. Allerdings können Sie die Umsetzung und tatsächliche Sicherheit dieser Maßnahmen nicht überprüfen, wenn der Schlüssel zum Entschlüsseln beim Cloud-Anbieter liegt. Die derzeit sicherste Variante ist daher, die Daten selbst zu verschlüsseln und anschließend in die Cloud zu übertragen. So können Sie sichergehen, dass nur Sie Zugriff auf Ihre Inhalte haben.

Das bedeutet jedoch auch, dass Sie Ihre Daten auf Ihrem Gerät ablegen und entschlüsseln müssen, um mit ihnen arbeiten zu können. Dazu ist es notwendig, dass auf jedem Gerät, mit dem Sie auf Ihre Inhalte zugreifen möchten, Ihr privater Schlüssel und die Verschlüsselungssoftware vorhanden sind. Ein gemeinschaftliches Arbeiten an Dokumenten in der Cloud ist unter diesen Umständen nicht mehr möglich.

10

Freigabe von Daten

Wenn Sie Daten in der Cloud mit anderen Personen teilen möchten, wird hierzu häufig eine Freigabe per Link eingerichtet. Dabei ist zu beachten, dass jede Person, die den Link kennt, Zugriff auf die freigegebenen Daten hat. Aus diesem Grund empfiehlt es sich, Freigaben möglichst zeitlich zu begrenzen. Außerdem sollten sie immer spezifisch und restriktiv angewendet werden. Sie könnten beispielsweise nur die benötigte Datei freigeben und nicht den gesamten Ordner, in dem die Datei liegt. Prüfen Sie zudem die Standardeinstellungen Ihres Cloud-Dienstes und passen Sie diese nach Ihren Bedürfnissen an.

11

Datenlöschung

Bevor Sie Ihre Daten einem Cloud-Anbieter anvertrauen, sollten Sie prüfen, wie aufwendig es ist, die Daten wieder aus der Cloud zu entfernen. Das endgültige Löschen von Daten in der Cloud gestaltet sich schwieriger als auf dem eigenen Rechner zu Hause. Cloud-Anbieter speichern zur Sicherheit oft mehrere Kopien der Dateien in verschiedenen Rechenzentren. Manche Cloud-Anbieter behalten die Daten auch nach einer Kündigung oder dem Löschen noch für einige Zeit für den Fall, dass die Kündigung zurückgenommen oder ein Nutzerkonto wieder aktiviert wird. Informationen hierzu finden Sie in den AGB des Dienstleisters. Gleichzeitig kann der Anbieter endgültig gelöschte Daten in der Regel nicht wiederherstellen. Für solche Fälle können Sie sich mit einer lokalen Datensicherung absichern.

Weiterführende Informationen

- Viele smarte Geräte lassen sich mit Cloud-Diensten verbinden. Informationen und Empfehlungen zum Thema Internet der Dinge und smarte Geräte finden Sie hier: bsi.bund.de/iot
- Viele Technologien, die gerade in der Entwicklung sind, basieren ebenfalls auf Cloud Computing. Ein Beispiel ist das vernetzte Fahren. Einen Überblick zu Risiken und Chancen dieser Technologie finden Sie hier: bsi.bund.de/vernetztes-fahren

Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Als unabhängige und neutrale Anlaufstelle bietet es Ihnen für einen sicheren digitalen Alltag umfangreiche Informationen.

IMPRESSUM

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsquelle:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi_bund
Service-Center: +49 (0) 800 274 1000

Stand: März 2021
Bilder: © GettyImages
Layout und Gestaltung: Faktor 3 AG

Artikelnummer: BSI-IFB 21/253